[eBooks] Open Source Intelligence Osint

Thank you completely much for downloading open source intelligence osint. Maybe you have knowledge that, people have look numerous period for their favorite books in the same way as this open source intelligence osint, but end happening in harmful downloads.

Rather than enjoying a good ebook subsequent to a cup of coffee in the afternoon, then again they juggled as soon as some harmful virus inside their computer. open source intelligence osint is welcoming in our digital library an online admission to it is set as public appropriately you can download it instantly. Our digital library saves in compound countries, allowing you to acquire the most less latency times to download any of our books behind this one. Merely said, the open source intelligence osint is universally compatible later any devices to read.

Automating Open Source Intelligence—Robert Layton 2015-12-03 Algorithms for Automating Open Source Intelligence (OSINT) 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 and 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 Methods and Tools—Nihad A. Hassan 2018-06-30 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 many 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 searching 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

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.

Handbook of Intelligence Studies—Loch K. Johnson 2007-01-24 This topical volume offers a comprehensive review of secret intelligence organizations and activities. Intelligence has been in the news consistently since 9/11 and the Iraqi WMD errors. Leading experts in the field approach the three major missions of intelligence: collection-and-analysis; covert action; and counterintelligence. Within each of these missions, the dynamically written essays dissect the so-called intelligence cycle to reveal the challenges of gathering and assessing information from around the world. Covert action, the most controversial intelligence activity, is explored, with special attention on the issue of military organizations moving into what was once primarily a civilian responsibility. The authors furthermore examine the problems that are associated with counterintelligence, protecting secrets from foreign spies and terrorist organizations, as well as the question of intelligence accountability, and how a nation can protect its citizens against the possible abuse of power by its own secret agencies. The Handbook of Intelligence Studies is a benchmark publication with major importance both for current research and for the future of the field. It is essential reading for advanced undergraduates, graduate students and scholars of intelligence studies, international security, strategic studies and political science in general.

Open Source Intelligence Techniques—Michael Bazzell 2016-04-29 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 techniques, you will learn how to locate: Hidden Social Network Content, Cell Phone Owner Information, Twitter GPS & Account Data, Hidden Photo GPS & Metadata, Deleted Websites & 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 Investigation—Babak Akhgari 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 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. 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 Investigation-Babak Ahkgar 2017-01-01 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. 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.

The Tao of Open Source Intelligence-Stewart Bertram 2015-04-23 OSINT is a rapidly evolving approach to intelligence collection, and its wide application makes it a useful methodology for numerous practices, including within the criminal investigation community. The Tao of Open Source Intelligence is your guide to the cutting edge of this information collection capability.

Open Source Intelligence in the Twenty-First Century-Christopher Hobbs 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.

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 crises and terrorism.

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.

Hacking Web Intelligence-Sudhanshu Chauhan 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 widely 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 hacking methods of obtaining information. Hacking Web Intelligence begins by introducing the basic 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, power searching 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. Covers 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.

Nowhere to Hide-Daniel Farber Huang 2021-03-26 Vibrantly illustrated, NOWHERE TO HIDE: Open Source Intelligence Gathering provides practical insight into the investigative tools and open source intelligence gathering (commonly known as “OSINT”) used by law enforcement, the media, and the general public to identify individuals involved in the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC. NOWHERE TO HIDE retraces the FBI’s investigative techniques - some using cutting-edge technology and others using old fashioned, knocking-on-doors detective work - used to pursue the hundreds of thousands of leads received from the general public. NOWHERE TO HIDE is filled with real world case studies, specific resources and practical “how to” guides to equip both beginner and seasoned OSINT investigators with the right tools for their OSINT toolboxes. This insightful volume includes 36 case studies that follow the FBI’s investigations of individual persons of interest, including the tactics, techniques, and procedures used by law enforcement, the media, and public sleuths to track down, identify, and - most importantly - verify the identities of suspected rioters. Learn how the FBI sifted through hundreds of thousands of leads, false positives, dead ends, as well as numerous unexpected leads to perform their investigations. NOWHERE TO HIDE provides vivid context around the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC, which left five people - one police officer and four protesters - dead by the end of the assault. Effective OSINT research requires a combination of technical knowledge to find the Who, What, When, Where, and How threads of data and information as well as taking into account our unpredictable human nature that sometimes leads us to do the things we do (the Why). OSINT is both science and art. NOWHERE TO HIDE provides practical, actionable information to help both individual and corporate investigators, researchers, advocates, and journalists navigate and penetrate OSINT resources to find the information and evidence they seek. Daniel Farber Huang is author of “Practical Cyber Security for Extremely Busy People” and a consultant to a wide range of organizations on cyber and strategy issues. He has worked closely with numerous federal, state, and local law enforcement agencies across the U.S. on providing solutions to their mobile technology requirements. He has focused on providing hardware and software solutions to federal field agents, investigators, the police, and other authorities to support them in performing their duties. He is a strategic consultant helping a wide range of companies in different industries reduce risks at all levels of their organizations, including their cyber security. Daniel is also a documentary photographer and freelance journalist.

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 mining, machine learning and predictive analytics combined with natural language processing and social network analysis to detect, disrupt, and neutralize cyber and physical threats. Chapters contain state-of-the-art social
media analytics and open source intelligence research trends. This multidisciplinary volume will appeal to students, researchers, and professionals working in the fields of open source intelligence, cyber crime and social network analytics. Chapter Automated Text Analysis for Intelligence Purposes: A Psychological Operations Case Study is available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

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


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

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 Atlas Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming 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 Vehicle Registration Details

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 modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interoperability 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 that are continually evolving beyond what we knew yesterday. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) 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.

The U.S. Intelligence Community—Jeffrey T Richelson 2018-05-04 The role of intelligence in US government operations has changed dramatically and is now more critical than ever to domestic security and foreign policy. This authoritative and highly researched book written by Jeffrey T. Richelson provides a detailed overview of America’s vast intelligence empire, from its organizations and operations to its management structure. Drawing from a multitude of sources, including hundreds of official documents, The US Intelligence Community allows students to understand the full scope of intelligence organizations and activities, and gives valuable support to policymakers and military operations. The seventh edition has been fully revised to include a new chapter on the major issues confronting the intelligence community, including secrecy and leaks, domestic spying, and congressional oversight, as well as revamped chapters on signals intelligence and cyber collection, geographic intelligence, and open sources. The inclusion of more maps, tables and photos, as well as electronic briefing books on the book’s Web site, makes The US Intelligence Community an even more valuable and engaging resource for students.

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?

The Five Disciplines of Intelligence Collection—Mark M. Lowenthal 2015-01-14 Leading intelligence experts Mark M. Lowenthal and Robert M. Clark bring together an all new, groundbreaking title. The Five Disciplines of Intelligence Collection describes, in non-technical terms, the definition, history, process, management, and future trends of each intelligence collection source (INT). Authoritative and non-political, this book is the perfect teaching tool for classes addressing various types of collection. Chapter authors are past or current senior practitioners of the INT they discuss, providing expert assessment of ways particular types of collection fit within the larger context of the U.S. Intelligence Community. This volume shows all-source analysts a full picture of how
Open Source Intelligence (OSINT) Link Directory-E. Ben Benavides 2010

The Oxford Handbook of National Security Intelligence-Loch K. Johnson 2010-03-12 The Oxford Handbook of National Security Intelligence is a state-of-the-art work on intelligence and national security. Edited by Loch Johnson, one of the world’s leading authorities on the subject, the handbook examines the topic in full, beginning with an examination of the major theories of intelligence. It then shifts its focus to how intelligence agencies operate, how they collect information from around the world, the problems that come with transforming “raw” information into credible analysis, and the difficulties in disseminating intelligence to policymakers. It also considers the balance between secrecy and public accountability, and the ethical dilemmas that covert and counterintelligence operations routinely present to intelligence agencies. Throughout, contributors factor in broader historical and political contexts that are integral to understanding how intelligence agencies function in our information-dominated age. The book is organized into the following sections: theories and methods of intelligence studies; historical background; the collection and processing of intelligence; the analysis and production of intelligence; the challenges of intelligence dissemination; counterintelligence and counterterrorism; covert action; intelligence and accountability; and strategic intelligence in other nations.

No Safe Haven-K. Hudnall Robert 2004-10 The terrorist attacks of September 11, 2001 marked the first time since Pancho Villa’s raid on Columbus, New Mexico that an enemy has attacked an American city. Was this just a fluke or a sign of things to come? Just how safe are the Borders of the United States? For the first time an author with a background in urban warfare and counter terrorism shows the true state of border security. Are we secure or a target waiting for a marksman? Find out the truth in No Safe Haven: Homeland Insecurity.

Down the Rabbit Hole an Osint Journey-Chris Kubecka 2017-06-29 Do you find 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. Analyse network and email configurations for entry points and exploits with FOCA, Maltego, Nmap/ZenMap, and Spiderfoot. Learn how to use advanced searches, 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 recon capabilities. 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 nijified 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 target 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.

Open Source Intelligence in a Networked World-Antony 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 this 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.

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.

Extreme Privacy-Michael Bazzell 2019 “This textbook is PROACTIVE. It is about starting over. It is the complete guide that I would give to any new client in an extreme situation. It leaves nothing out and provides explicit details of every step I take to make someone completely disappear, including document templates and a chronological order of events. The information shared in this book is based on real experiences with my actual clients, and is unlike any content ever released in my other books.” — publisher.

Open Source Intelligence (OSINT)- 2007

Intelligence and Security Informatics-Paul Kantor 2005-05-12 This book constitutes the refereed proceedings of the IEEE International Conference on Intelligence and Security Informatics, ISI 2005, held in Atlanta, GA, USA in May 2005. The 28 revised full papers, 34 revised short papers, and 32 poster abstracts presented were carefully reviewed and selected for inclusion in the book. The papers are organized in topical sections on data and text mining, infrastructure protection and emergency response, information management and security education, deception detection and authorship analysis, monitoring and surveillance, and terrorism informatics.

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) inside out from multiple perspectives, including those of hackers and seasoned intelligence 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 commentary. 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 CIS0/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.
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 introduces readers to the tools Bellingcat investigators use, tools available to anyone, from software that helps 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.


Intelligence and the National Security Strategist - Roger Z. George 2006 Presents students with an anthology of published articles from diverse sources as well as contributions to the study of intelligence. This collection includes perspectives from the history of warfare, views on the evolution of US intelligence, and studies on the balance between the need for information-gathering and the values of a democracy.” - publisher.

Application of Social Media in Crisis Management - Babak Akhgar 2017-03-27 This book explores how social media and its advances enables citizens to empower themselves during a crisis. The book addresses the key issues related to crises management and social media as the new platform to assist citizens and first responders dealing with multiple forms of crisis from major terrorist attacks, larger scale public disorder, large-scale movement of people across borders, and natural disasters. The book is based on the results and knowledge gained during the European Commission ATHENA project which has been addressing critical issues in contemporary crisis management and social media and smart mobile communications. This book is authored by a mix of global contributors from across the landscape of academia, emergency response and experts in government policy and private industry. This title explores and explains that during a modern crisis, the public self-organizes into voluntary groups, adapt quickly to changing circumstances, emerge as leaders and experts and perform life-saving actions; and that they are increasingly reliant upon the use of new communications media to do it.

Open Source Intelligence (OSINT): Issues for Congress - 2007 Open source information (OSINT) is derived from newspapers, journals, radio and television, and the Internet. Intelligence analysts have long used such information to supplement classified data, but systematically collecting open source information has not been a priority of the U.S. Intelligence Community (IC). In recent years, given changes in the international environment, there have been calls, from Congress and the 9/11 Commission among others, for a more intense and focused investment in open source collection and analysis. However, some still emphasize that the primary business of intelligence continues to be obtaining and analyzing secrets.


Automating Open Source Intelligence - Robert Layton 2015-11-15 Algorithms for Automating Open Source Intelligence (OSINT) 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

Enabling Open Source Intelligence (OSINT) in Private Social Networks - Benjamin Robert Holland 2012