Open Source Intelligence Course Osint

From Strategy to Implementation
Hunting Cyber Criminals
Counterterrorism and Open Source Intelligence
Automating Open Source Intelligence
The Oxford Handbook of National Security Intelligence
Hacking Web Intelligence
What it Takes to Disappear in America
A Practical Guide to Online Intelligence
Global Information Warfare
First Asia-Pacific Conference, WI 2001, Maebashi City, Japan, October 23-26, 2001, Proceedings
Fixing the Spy Machine
A Primer for the Ethical Hacker
How action-based intelligence can be an effective response to incidents
Publications Combined: Studies In Open Source Intelligence (OSINT) And Information
A Hacker's Guide to Online Intelligence Gathering Tools and Techniques
Open Source Intelligence Techniques
Achieving Asymmetric Advantage in the Face of Nontraditional Threats
Python Programming for Hackers and Reverse Engineers
Open Source Intelligence and Web Reconnaissance Concepts and Techniques
Digital Witness
More Autonomous and Diverse--within Limits: an Intelligence Monograph
A Guide for the Serious Searcher
Practical Social Engineering
Google Hacking for Penetration Testers
Extreme Privacy
The New Craft of Intelligence

Internet Searches for Vetting, Investigations, and Open-Source Intelligence
A Practical Guide to Online Intelligence
Eliminating Personal Online Information
Web Intelligence: Research and Development
Open Source Intelligence Tools and Resources Handbook
A Question Of Trust
Preparing American Intelligence for the Twenty-first Century
Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism
Resources for Searching and Analyzing Online Information
Intelligence Issues and Developments
Algorithms for OSINT
מימצאי סקר רעיונות של אנשי שדה ואקדמיה לפרוייקט חינוכי מרכזי באזורי מצוקה
Open Source Intelligence Methods and Tools
Open Source Intelligence Methods and Tools

SINGLETON MORA

From Strategy to Implementation ABC-CLIO
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.
Hunting Cyber Criminals No Starch Press
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 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, 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

Counterterrorism and Open Source Intelligence Springer Science & Business Media

Internet Intelligence & Investigation is a powerful tool against crime, however, the collection of internet data and information is heavily regulated. Improper use of the internet for investigative purposes can put an investigator and their employer at physical, financial and legal risk. Therefore, it is vital that legal and ethical standards are followed when conducting investigative activity online. The Internet Intelligence and Investigation Handbook details the professional standards that are vital to conducting investigative activity online. Criminal and Security Intelligence specialist Steve Adams presents knowledge and advice that will ensure that any internet-based investigative activity that you conduct is carried out in a legal and ethical way that guarantees the rights of the subject and ensures your legal and physical safety. This handbook details best practice for both public sector and private sector organisations. Standards adopted when conducting investigative activity online within the public and private sectors are inconsistent, risking the integrity of investigations and prosecutions. This document is designed to be relied on by organisations industrywide to establish a consistent and modern standard for the conducting of Internet Intelligence & Investigation activity.

Automating Open Source Intelligence IGI Global
SCOTT (copy 1): From the John Holmes Library collection.
The Oxford Handbook of National Security Intelligence John Wiley & Sons
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.
Hacking Web Intelligence IT Governance Ltd
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
What it Takes to Disappear in America Syngress
This book constitutes the refereed proceedings of the First Asia-Pacific Conference on Web Intelligence, WI 2001, held in Maebashi City, Japan, in October 2001.The 28 revised full papers and 45 revised short papers presented were carefully reviewed and selected from 153 full-length paper submissions. Also included are an introductory survey and six invited presentations. The book offers topical sections on Web information systems environments and foundations, Web human-media engineering, Web information management, Web information retrieval, Web agents, Web mining and farming, and Web-based applications.
A Practical Guide to Online Intelligence No Starch Press
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.
Global Information Warfare Oxford University Press, USA
"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.
First Asia-Pacific Conference, WI 2001, Maebashi City, Japan, October 23-26, 2001, Proceedings Nova Publishers
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.
Fixing the Spy Machine Jeffrey Frank Jones
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?
A Primer for the Ethical Hacker Apress
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

How action-based intelligence can be an effective response to incidents DIANE Publishing

The U.S. Intelligence Community continues to adjust to the 21st Century environment. In the post-Cold War world, terrorism, narcotics trafficking and related money laundering is perceived both as criminal matters and as threats to the nation's security. Priority continues to be placed on intelligence support to military operations and on involvement in efforts to combat transnational threats, especially international terrorism. Growing concerns about transnational threats are leading to increasingly close co-operation between intelligence and law enforcement agencies. This book presents new in-depth analyses of developments in the field.

Publications Combined: Studies In Open Source Intelligence (OSINT) And Information CRC Press

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.

A Hacker's Guide to Online Intelligence Gathering Tools and Techniques Springer

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 protocol 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.

Open Source Intelligence Techniques Createspace Independent Publishing Platform

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.

Achieving Asymmetric Advantage in the Face of Nontraditional Threats Syngress

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 issued for public and private 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 reviews relevant laws, regulations, and rulings as they pertain to Internet crimes, misbehaviors, and individuals’ privacy. Exploring technologies such as social media and aggregate information services, the author outlines the techniques and skills that can be used to leverage the capabilities of networked systems on the Internet and find critically important data to complete an up-to-date picture of people, employees, entities, and their activities. Outlining appropriate adoption of legal, policy, and procedural principles—and emphasizing the careful and appropriate use of Internet searching within the law—the book includes coverage of cases, privacy issues, 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.

Python Programming for Hackers and Reverse Engineers CRC Press

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-polemical, 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 to better task and collaborate with their collection partners, and gives intelligence collectors an appreciation of what happens beyond their "stovepipes," as well as a clear assessment of the capabilities and limitations of INT collection.

Open Source Intelligence and Web Reconnaissance Concepts and Techniques Packt Publishing Ltd

When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen? In Black Hat Python, the latest from Justin Seitz (author of the best-selling Gray Hat Python), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You'll learn how to: –Create a trojan command-and-control using GitHub –Detect sandboxing and automate common malware tasks, like keylogging and screenshotting –Escalate Windows privileges with creative process control –Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine –Extend the popular Burp Suite web-hacking tool –Abuse Windows COM automation to perform a man-in-the-browser attack –Exfiltrate data from a network most sneakily Insider techniques and creative challenges throughout show you how to extend the hacks and how to write your own exploits. When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in Black Hat Python. Uses Python 2

Digital Witness Lulu.com

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.