Open Source Intelligence Techniques: Resources For Searching And Analyzing Online Information

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.

New 2018 Fourth Edition Take control of your privacy by removing your personal information from the internet with this updated Fourth Edition. Author Michael Bazzell has been well known in government circles for his ability to locate personal information about anyone through the internet. In Hiding from the Internet: Eliminating Personal Online Information, he exposes the resources that broadcast your personal details to public view. He has researched each source and identified the best method to have your private details removed from the databases that store profiles on all of us. This book will serve as a reference guide for anyone that values privacy. Each technique is explained in simple steps. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The author provides personal experiences from his journey to disappear from public view. 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 force companies to remove you from their data collection systems. This book exposes loopholes that create unique opportunities for privacy seekers. Among other techniques, you will learn to: Remove your personal information from public databases and people search sites Create free anonymous mail addresses, email addresses, and telephone numbers Control your privacy settings on social networks and remove sensitive data Provide disinformation to conceal true private details Force data brokers to stop sharing your information with both private and public organizations Prevent marketing companies from monitoring your browsing, searching, and shopping habits Remove your landline and cellular telephone numbers from online websites Use a credit freeze to eliminate the worry of financial identity theft and fraud Change your future habits to promote complete privacy and anonymity Conduct a complete background check to verify proper information removal Configure a home firewall with VPN Kill-Switch Purchase a completely invisible home or vehicle

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.

An exploration of why we play video games despite the fact that we are almost certain to feel unhappy when we fail at them. We may think of video games as being "fun," but in The Art of Failure, Jesper Juul claims that this is almost entirely mistaken. When we play video games, our facial expressions are rarely those of happiness or bliss. Instead, we frown, grimace, and shout in frustration as we lose, or die, or fail to advance to the next level. Humans may have a fundamental desire to succeed and feel competent, but game players choose to engage in an activity in which they are nearly certain to fail and feel incompetent. So why

do we play video games even though they make us unhappy? Juul examines this paradox. In video games, as in tragic works of art, literature, theater, and cinema, it seems that we want to experience unpleasantness even if we also dislike it. Reader or audience reaction to tragedy is often explained as catharsis, as a purging of negative emotions. But, Juul points out, this doesn't seem to be the case for video game players. Games do not purge us of unpleasant emotions; they produce them in the first place. What, then, does failure in video game playing do? Juul argues that failure in a game is unique in that when you fail in a game, you (not a character) are in some way inadequate. Yet games also motivate us to play more, in order to escape that inadequacy, and the feeling of escaping failure (often by improving skills) is a central enjoyment of games. Games, writes Juul, are the art of failure: the singular art form that sets us up for failure and allows us to experience it and experiment with it. The Art of Failure is essential reading for anyone interested in video games, whether as entertainment, art, or education.

Resources for Searching and Analyzing Online Information

World Social Report 2020

Digital

Open Source Intelligence Methods and Tools

Internet Searches for Vetting, Investigations, and Open-Source Intelligence

Hacking Web Intelligence

Algorithms for OSINT

A fully revised and updated edition of the bible of the newspaper industry

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.

This book covers the developing field of open source research and discusses how to use social media, satellite imagery, big data analytics, and user-generated content to strengthen human rights research and investigations. The topics are presented in an accessible format through extensive use of images and data visualization (éditeur).

Get to grips with cyber threat intelligence and data-driven threat hunting while exploring expert tips and techniques Key

FeaturesSet up an environment to centralize all data in an Elasticsearch, Logstash, and Kibana (ELK) server that enables threat huntingCarry out atomic hunts to start the threat hunting process and understand the environmentPerform advanced hunting using MITRE ATT&CK Evals emulations and Mordor datasetsBook Description Threat hunting (TH) provides cybersecurity analysts and enterprises with the opportunity to proactively defend themselves by getting ahead of threats before they can cause major damage to their business. This book is not only an introduction for those who don't know much about the cyber threat intelligence (CTI) and TH world, but also a guide for those with more advanced knowledge of other cybersecurity fields who are looking to implement a TH program from scratch. You will start by exploring what threat intelligence is and how it can be used to detect and prevent cyber threats. As you progress, you'll learn how to collect data, along with understanding it by developing data models. The book will also show you how to set up an environment for TH using open source tools. Later, you will focus on how to plan a hunt with practical examples, before going on to explore the MITRE ATT&CK framework. By the end of this book, you'll have the skills you need to be able to carry out effective hunts in your own environment. What you will learnUnderstand what CTI is, its key concepts, and how it is useful for preventing threats and protecting your organizationExplore the different stages of the TH processModel the data collected and understand how to document the findingsSimulate threat actor activity in a lab environmentUse the information collected to detect breaches and validate the results of your queriesUse documentation and strategies to communicate processes to senior management and the wider businessWho this book is for If you are looking to start out in the cyber intelligence and threat hunting domains and want to know more about how to implement a threat hunting division with open-source tools, then this cyber threat intelligence book is for you.

Eliminating Personal Online Information

The Science of Human Hacking

Resources for Searching and Analyzing Online Information (le)

Open Source Intelligence Techniques

A Technical Guide

Operator Handbook

Inequality in a Rapidly Changing World

Capitalist Nigger is an explosive and jarring indictment of the black race. The book asserts that the Negroid race, as naturally endowed as any other, is culpably a non-productive race, a consumer race that depends on other communities for its culture, its language, its feeding and its clothing. Despite enormous natural resources, blacks are economic slaves because they lack the ‘devil-may-care’ attitude and the ‘killer instinct’ of the Caucasian, as well as the spider web mentality of the Asian. A Capitalist Nigger must embody ruthlessness in pursuit of excellence in his drive towards achieving the goal of becoming an economic warrior. In putting forward the idea of the Capitalist Nigger, Chika Onyeani charts a road to success whereby black economic warriors employ the ‘Spider Web Doctrine’ - discipline, self-reliance, ruthlessness - to escape from their victim mentality. Born in Nigeria, Chika

Onyeani is a journalist, editor and former diplomat.

Provides an unclassified reference handbook which explains the categories of intelligence threat, provides an overview of worldwide threats in each category, and identifies available resources for obtaining threat information. Contents: intelligence collection activities and disciplines (computer intrusion, etc.); adversary foreign intelligence operations (Russian, Chinese, Cuban, North Korean and Romanian); terrorist intelligence operations; economic collections directed against the U.S. (industrial espionage); open source collection; the changing threat and OPSEC programs.

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

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.

What it Takes to Disappear in America

Cybersecurity Blue Team Toolkit

Introduction to Intelligence Studies

Open Source Intelligence Gathering for Penetration Testing

Social Media Analytics

The Art of Failure

Structured Analytic Techniques for Intelligence Analysis

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.

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, iOS, 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.

Third Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected 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 sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, 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 improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Owner InformationTwitter GPS & Account DataHidden Photo GPS & MetadataDeleted Websites & PostsWebsite Owner InformationAlias Social Network ProfilesAdditional User AccountsSensitive Documents & PhotosLive Streaming Social ContentIP Addresses of UsersNewspaper Archives & ScansSocial Content by LocationPrivate Email AddressesHistorical Satellite ImageryDuplicate Copies of PhotosLocal Personal Radio FrequenciesCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsComplete Facebook DataFree Investigative SoftwareAlternative Search EnginesStolen Items for SaleUnlisted AddressesUnlisted Phone NumbersPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal Activity

In this Second Edition of Structured Analytic Techniques for Intelligence Analysis, authors Richards J. Heuer Jr. and Randolph H. Pherson showcase fifty-five structured analytic techniques—five new to this edition—that represent the most current best practices in intelligence, law enforcement, homeland security, and business analysis.

A Practical Guide to Internet Investigation

The Internet Intelligence & Investigation Handbook

Digital Witness

From Strategy to Implementation

How to Find Out Anything

Intelligence Threat Handbook

The Road To Success – A Spider Web Doctrine

This report examines the links between inequality and other major global trends (or megatrends), with a focus on technological change, climate change, urbanization and international migration. The analysis pays particular attention to poverty and labour market trends, as they mediate the distributional impacts of the major trends selected. It also provides policy recommendations to manage these megatrends in an equitable manner and considers the policy implications, so as to reduce inequalities and support their implementation.

Fifth Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected 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 sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, 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 improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details
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 Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, he shares his methods in great detail. Each step of his process is explained throughout twenty-four 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 ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationAutomated Collection SolutionsLinux Investigative ProgramsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details
Since the attacks of 9/11, the United States Intelligence Community (IC) has undergone an extensive overhaul.

Perhaps the greatest of these changes has been the formation of the Office of the Director of National Intelligence. As a cabinet-level official, the Director oversees the various agencies of the IC and reports directly to the President. The IC today faces challenges as it never has before; everything from terrorism to pandemics to economic stability has now become an intelligence issue. As a result, the IC is shifting its focus to a world in which tech-savvy domestic and international terrorists, transnational criminal organizations, failing states, and economic instability are now a way of life. Introduction to Intelligence Studies provides a comprehensive overview of intelligence and security issues, defining critical terms, and reviewing the history of intelligence as practiced in the United States. Designed in a practical sequence, the book begins with the basics of intelligence, progresses through its history, describes best practices, and explores the way the IC looks and operates today. Each chapter begins with objectives and key terms and closes with questions to test reader assimilation. The authors examine the "pillars" of the American intelligence system—collection, analysis, counterintelligence, and covert operations—and demonstrate how these work together to provide "decision advantage." The book provides equal treatment to the functions of the intelligence world—balancing coverage on intelligence collection, counterintelligence, information management, critical thinking, and decision-making. It also covers such vital issues as laws and ethics, writing and briefing for the IC, and the emerging threats and challenges that intelligence professionals will face in the future.

Dialogues at the Economic and Social Council

Open Source Intelligence Tools and Resources Handbook

Social Engineering

Purple Team Field Manual

Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise

Hiding from the Internet

Resources for Searching and Analyzing Online Information (LEIU)

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. 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 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 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.

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.

Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire—why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the "system" in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer's bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don't work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer's playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.

This report includes an analytic assessment drafted and coordinated among The Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which draws on intelligence information collected and disseminated

by those three agencies. It covers the motivation and scope of Moscow's intentions regarding US elections and Moscow's use of cyber tools and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the 2016 US presidential election and draws on our understanding of previous Russian influence operations. When we use the term "we" it refers to an assessment by all three agencies. * This report is a declassified version of a highly classified assessment. This document's conclusions are identical to the highly classified assessment, but this document does not include the full supporting information, including specific intelligence on key elements of the influence campaign. Given the redactions, we made minor edits purely for readability and flow. We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or US public opinion. * New information continues to emerge, providing increased insight into Russian activities. * PHOTOS REMOVED

A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools

Open Source Intelligence and Web Reconnaissance Concepts and Techniques

Open Source Intelligence and Cyber Crime

Hunting Cyber Criminals

Red Team + OSINT + Blue Team Reference

The Complete Privacy & Security Desk Reference

Open Source Intelligence Investigation

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.

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 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.

Open Source Intelligence TechniquesResources for Searching and Analyzing Online Information

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 vast, yet little-known online resources that search engines cannot scour, such as refdesk.com, ipl.org, the University of Michigan Documents Center, and Project Gutenberg, among many others. •How to access free government resources (and put your tax dollars to good use). •How to find experts and other people with special knowledge. •How to dig up seemingly confidential information on people and businesses, from public and private companies to non-profits and international companies. Whether researching for a term paper or digging up dirt on an ex, the advice in this book arms you with the sleuthing skills to tackle any mystery.

Resources for Searching and Analyzying Online Information

This Book Was Self-Published

The Tao of Open Source Intelligence

Down the Rabbit Hole an Osint Journey

From Extreme Google Searches to Scouring Government Documents, a Guide to Uncovering Anything About Everyone and Everything

An Essay on the Pain of Playing Video Games

Using Open Source Information for Human Rights Investigation, Documentation, and Accountability

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection

and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracert, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions •Straightforward explanations of the theory behind cybersecurity best practices •Designed to be an easily navigated tool for daily use •Includes training appendix on Linux, how to build a virtual lab and glossary of key terms The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

There is no shortage of books about becoming a self-published author. Most titles try to motivate you to write your novel, focus on marketing strategies, and explore the occasional self-made millionaire success story. This is not that type of book. This is a technical manual. It identifies the benefits and risks of choosing Expanded Distribution for a project and the limitations of Independently Published titles issued exclusively by Amazon. It clearly explains the nuances of free and paid ISBNs and the strategy of using both to ensure titles are available to every library and bookstore in the world, while maximizing royalties for copies sold on Amazon. It explains the differences between standard PDF files and PDF/X-1a:2001 formats, and reasons why the latter is the best to use for final proof-ready documents. It includes all of the details the author wishes he would have known before starting his self-publishing journey throughout eighteen published books. The technical formalities of creating your own book are missing from the other titles in this space, and likely the reason many people never see their work make it to publication. This book removes the mysteries surrounding hardware configuration, software requirements, document formatting, book content, print publishing, E-book publishing, audiobook publishing, podcast publishing, book piracy, marketing, promotion, affiliate programs, income monitoring, tax reporting, and every other issue related to your own publication process. This book lays out all of the author's experiences and how he chooses from the platforms available for distribution. The entire book was written while executing the steps which are discussed. While documenting the formatting of each chapter, the book itself is altered in real-time. All experiences are documented chronologically. As you read along, you experience frustrations and failures together with the author. All encountered issues are resolved before proceeding to the next task, and all templates are available for download. Simply stated, this book is about this book. It provides a unique experience which allows you to make it through the nuances of self-publishing.

"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) 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

Achieving Sustainable Development and Promoting Development Cooperation

Automating Open Source Intelligence

Capitalist Nigger

Google Hacking for Penetration Testers

PTFM

A Practical Guide to Online Intelligence

Extreme Privacy

This 500-page textbook will explain how to become digitally invisible. You will make all of your communications private, data encrypted, internet connections anonymous, computers hardened, identity guarded, purchases secret, accounts secured, devices locked, and home address hidden. You will remove all personal information from public view and will reclaim your right to privacy. You will no longer give away your intimate details and you will take yourself out of 'the system'. You will use covert aliases and misinformation to eliminate current and future threats toward your privacy & security. When taken to the extreme, you will be impossible to compromise.

This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 8/05). But, Google's search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google used by security professionals and system administrators to find this sensitive information and "self-police their own organizations. Readers will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can "mash up" Google with MySpace, LinkedIn, and more for passive reconaissance. • Learn Google Searching Basics Explore Google's Web-based Interface, build Google queries, and work with Google URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators

and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding and Database Digging See the ways to use Google to locate documents and then search within the documents to locate information. • Understand Google's Part in an Information Collection Framework Learn the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple Security Searches Learn a few searches that give good results just about every time and are good for a security assessment. • Track Down Web Servers Locate and profile web servers, login portals, network hardware and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

This book presents an overview of the key debates that took place during the Economic and Social Council meetings at the 2007 High-level Segment, at which ECOSOC organized its first biennial Development Cooperation Forum. The discussions also revolved around the theme of the second Annual Ministerial Review, "Implementing the internationally agreed goals and commitments in regard to sustainable development."--P. 4 of cover.

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.

Counterterrorism and Open Source Intelligence

Practical Threat Intelligence and Data-Driven Threat Hunting

Assessing Russian Activities and Intentions in Recent Us Elections

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

The Associated Press Stylebook 2015

Red teams can show flaws that exist in your network before they are compromised by malicious actors and blue teams traditionally assess current security measures and identify security flaws. The teams can provide valuable feedback to each other, but this is often overlooked, enter the purple team. The purple team allows for the integration of red team tactics and blue team security measures. The purple team field manual is a manual for all security professionals and

integrates red and blue team methodologies.

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.

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