

Automating Open Source Intelligence

This book gathers the proceedings of the 2018 International Conference on Digital Science (DSIC'18), held in Budva, Montenegro, on October 19 – 21, 2018. DSIC'18 was an international forum for researchers and practitioners to present and discuss the latest innovations, trends, results, experiences and concerns in Digital Science. The main goal of the Conference was to efficiently disseminate original findings in the natural and social sciences, art & the humanities. The contributions address the following topics: Digital Agriculture & Food Technology Digital Art & Humanities Digital Economics Digital Education Digital Engineering Digital Environmental Sciences Digital Finance, Business & Banking Digital Health Care, Hospitals & Rehabilitation Digital Media Digital Medicine, Pharma & Public Health Digital Public Administration Digital Technology & Applied Sciences Digital Virtual Reality

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

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.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Learn Business Intelligence Markup Language (Biml) for automating much of the repetitive, manual labor involved in data integration. We teach you how to build frameworks and use advanced Biml features to get more out of SQL Server Integration Services (SSIS), Transact-SQL (T-SQL), and SQL Server Analysis Services (SSAS) than you ever thought possible. The first part of the book starts with the basics—getting your development environment configured, Biml syntax, and scripting essentials. Whether a beginner or a seasoned Biml expert, the next part of the book guides you through the process of using Biml to build a framework that captures both your design patterns and execution management. Design patterns are reusable code blocks that standardize the approach you use to perform certain types of data integration, logging, and other key data functions. Design patterns solve common problems encountered when developing data integration solutions. Because you do not have to build the code from scratch each time, design patterns improve your efficiency as a Biml developer. In addition to leveraging design patterns in your framework, you will learn how to build a robust metadata store and how to package your framework into Biml bundles for deployment within your enterprise. In the last part of the book, we teach you more advanced Biml features and capabilities, such as SSAS development, T-SQL recipes, documentation autogeneration, and Biml troubleshooting. The Biml Book: Provides practical and applicable examples Teaches you how to use Biml to reduce development time while improving quality Takes you through solutions to common data integration and BI challenges What You'll Learn Master the basics of Business Intelligence Markup Language (Biml) Study patterns for automating SSIS package generation Build a Biml Framework Import and transform database schemas Automate generation of scripts and projects Who This Book Is For BI developers wishing to quickly locate previously tested solutions, Microsoft BI specialists, those seeking more information about solution automation and code generation, and practitioners of Data Integration Lifecycle Management (DILM) in the DevOps enterprise

Open Source Data Warehousing and Business Intelligence is an all-in-one reference for developing open source based data warehousing (DW) and business intelligence (BI) solutions that are business-centric, cross-customer viable, cross-functional, cross-technology based, and enterprise-wide. Considering the entire lifecycle of an open source DW &

The present book includes extended and revised versions of papers presented during the 2018 International Computer Symposium (ICS 2018), held in Yunlin, Republic of China (Taiwan), on December 20-22, 2018. The 86 papers presented were carefully reviewed and selected from 263 submissions from 11 countries. The variety of the topics include machine learning, sensor devices and platforms, sensor networks, robotics, embedded systems, networks, operating systems, software system structures, database design and models, multimedia and multimodal retrieval, object detection, image processing, image compression, mobile and wireless security.

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.

[Conservation Research, Policy and Practice](#)

[Using Open Source Information for Human Rights Investigation, Documentation, and Accountability](#)

[Publications Combined: Studies In Open Source Intelligence \(OSINT\) And Information](#)

[Ten Strategies of a World-Class Cybersecurity Operations Center](#)

[A Collection of Innovative Research Case-studies that are Reworking the Way We Look at Industry 4.0 Thanks to Artificial Intelligence](#)

[Artificial Intelligence in Industry 4.0](#)

[Theories, Methods, Tools and Technologies](#)

[Secure your network with Kali Linux 2019.1 – the ultimate white hat hackers' toolkit, 3rd Edition](#)

[Resources for Searching and Analyzing Online Information](#)

[Introduction to Social Media Investigation](#)

[The Open-Source Everything Manifesto](#)

[Patterns and Paradigms for Scalable, Reliable Services](#)

[Open Source Data Warehousing and Business Intelligence](#)

Over the years since my first presentation involving OSINT, a lot has been said, discussed, and thrown around about it; in some cases with little regard for the understanding of the good, the bad, and the ugly, of OSINT. Also, with little consideration to understanding precisely what OSINT and other Intelligence categories are and can do.

Automating Open Source Intelligence Algorithms for OSINT Syngress

This book gathers selected papers presented at the Inventive Communication and Computational Technologies conference (ICICCT 2019), held on 29-30 April 2019 at Gnanamani College of Technology, Tamil Nadu, India. The respective contributions highlight recent research efforts and advances in a new paradigm called ISMAC (IoT in Social, Mobile, Analytics and Cloud contexts). Topics covered include the Internet of Things, Social Networks, Mobile Communications, Big Data Analytics, Bio-inspired Computing and Cloud Computing. The book is chiefly intended for academics and practitioners working to resolve practical issues in this area.

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigations Gather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10-specific feature forensics Utilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

The internet of things (IoT) is quickly growing into a large industry with a huge economic impact expected in the near future. However, the users' needs go beyond the existing web-like services, which do not provide satisfactory intelligence levels. Ambient intelligence services in IoT environments is an emerging research area that can change the way that technology and services are perceived by the users. Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities is a unique source that systemizes recent trends and advances for service development with such key technological

enablers of modern ICT as ambient intelligence, IoT, web of things, and cyber-physical systems. The considered concepts and models are presented using a smart spaces approach with a particular focus on the Smart-M3 platform, which is now shaping into an open source technology for creating ontology-based smart spaces and is shifting towards the development of web of things applications and socio-cyber-physical systems. Containing coverage on a broad range of topics such as fog computing, smart environments, and virtual reality, multitudes of researchers, students, academicians, and professionals will benefit from this timely reference.

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, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented 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.

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?

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.

[Business Intelligence and Data Warehouse Automation](#)

[Complete guide to automating Big Data solutions using Artificial Intelligence techniques](#)

[Artificial Intelligence for Big Data](#)

[Gray Hat Python](#)

[Open Source Intelligence Techniques](#)

[Social Media Analytics](#)

[New Trends in Computer Technologies and Applications](#)

[The Biml Book](#)

[A Practical Guide to Online Intelligence](#)

[International Workshop, BioSecure 2008, Raleigh, NC, USA, December 2, 2008. Proceedings](#)

[Algorithms for Osint](#)

[Digital Science](#)

What the world lacks right now—especially the United States, where every form of organization from government to banks to labor unions has betrayed the public trust—is integrity. Also lacking is public intelligence in the sense of decision-support: knowing what one needs to know in order to make honest decisions for the good of all, rather than corrupt decisions for the good of the few. The Open-Source Everything Manifesto is a distillation of author, strategist, analyst, and reformer Robert David Steele life's work: the transition from top-down secret command and control to a world of bottom-up, consensual, collective decision-making as a means to solve the major crises facing our world today. The book is intended to be a catalyst for citizen dialog and deliberation, and for inspiring the continued evolution of a nation in which all citizens realize our shared aspiration of direct democracy—informed participatory democracy. Open-Source Everything is a cultural and philosophical concept that is essential to creating a prosperous world at peace, a world that works for one hundred percent of humanity. The future of intelligence is not secret, not federal, and not expensive. It is about transparency, truth, and trust among our local to global collective. Only "open" is scalable. As we strive to recover from the closed world corruption and secrecy that has enabled massive fraud within governments, banks, corporations, and even non-profits and universities, this timely book is a manifesto for liberation—not just open technology, but open everything.

Build next-generation Artificial Intelligence systems with Java Key Features Implement AI techniques to build smart applications using Deeplearning4j Perform big data analytics to derive quality insights using Spark MLlib Create self-learning systems using neural networks, NLP, and reinforcement learning Book Description In this age of big data, companies have larger amount of consumer data than ever before, far more than what the current technologies can ever hope to keep up with. However, Artificial Intelligence closes the gap by moving past human limitations in order to analyze data. With the help of Artificial Intelligence for big data, you will learn to use Machine Learning algorithms such as k-means, SVM, RBF, and regression to perform advanced data analysis. You will understand the current status of Machine and Deep Learning techniques to work on Genetic and Neuro-Fuzzy algorithms. In addition, you will explore how to develop Artificial Intelligence algorithms to learn from data, why they are necessary, and how they can help solve real-world problems. By the end of this book, you'll have learned how to implement various Artificial Intelligence algorithms for your big data systems and integrate them into your product offerings such as reinforcement learning, natural language processing, image recognition, genetic algorithms, and fuzzy logic systems. What you will learn Manage Artificial Intelligence techniques for big data with Java Build smart systems to analyze data for enhanced customer experience Learn to use Artificial Intelligence frameworks for big data Understand complex problems with algorithms and Neuro-Fuzzy systems Design stratagems to leverage data using Machine Learning process Apply Deep Learning techniques to prepare data for modeling Construct models that learn from data using open source tools Analyze big data problems using scalable Machine Learning algorithms Who this book is for This book is for you if you are a data scientist, big data professional, or novice who has basic knowledge of big data and wish to get proficiency in Artificial Intelligence techniques for big data. Some competence in mathematics is an added advantage in the field of elementary linear algebra and calculus.

Completely Rewritten Sixth Edition Sheds New Light on Open Source Intelligence Collection and Analysis Author Michael Bazzell has been well known in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout twenty-five chapters of specialized websites, software solutions, and creative search techniques. Over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will greatly improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Subscriber Information Deleted Websites & Posts Missing Facebook Profile Data Full Twitter Account Data Alias Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming Social Content Social Content by Location IP Addresses of Users Additional User Accounts Sensitive Documents & Photos Private Email Addresses Duplicate Video Posts Mobile App Network Data Unlisted Addresses &#s 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

This new resource presents the principles and applications in the emerging discipline of Activity-Based Intelligence (ABI). This book will define, clarify, and demystify the tradecraft of ABI by providing concise definitions, clear examples, and thoughtful discussion. Concepts, methods, technologies, and applications of ABI have been developed by and for the intelligence community and in this book you will gain an understanding of ABI principles and be able to apply them to activity based intelligence analysis. The book is intended for intelligence professionals, researchers, intelligence studies, policy makers, government staffers, and industry representatives. This book will help practicing professionals understand ABI and how it can be applied to real-world problems.

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.

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.

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.

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.

[Spies and Secrecy in an Open World](#)

[Open Source Intelligence Methods and Tools](#)

[Designing Distributed Systems](#)

[Transparency, Truth, and Trust](#)

[Python Programming for Hackers and Reverse Engineers](#)

[Machine Learning and Security](#)

[Algorithms for OSINT](#)

[Hunting Cyber Criminals](#)

[Biosurveillance and Biosecurity](#)

[Mastering Kali Linux for Advanced Penetration Testing](#)

[Defining Second Generation Open Source Intelligence \(Osint\) for the Defense Enterprise](#)

[Protecting Systems with Data and Algorithms](#)

[Open Source Intelligence Tools and Resources Handbook](#)

J.

'Kevin Roose provides a clear, compelling strategy for surviving the next wave of technology with our jobs - and souls - intact... Futureproof is the survival guide you need' Charles Duhigg, The Power of Habit In this timely, counterintuitive, and highly practical guide to the age of A.I. and automation, a New York Times technology columnist argues that the key to success is making yourself more human, not less. The machines are here. After decades of sci-fi doomsaying and marketing hype, advanced A.I. and automation technologies have leapt out of research labs and Silicon Valley engineering departments and into the center of our lives. The world's biggest corporations are racing to automate jobs, and some experts predict that A.I could put millions of people out of work. But all is not lost. With a little effort, we can become futureproof. In Futureproof: 9 Rules for Machine-Age Humans, New York Times technology columnist Kevin Roose lays out an optimistic vision of how people can thrive in the machine age by rethinking their relationship with technology, and making themselves irreplaceably human.

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine's Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT): Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media: Valuable Tools in Today's Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS

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

In the race to compete in today's fast-moving markets, large enterprises are busy adopting new technologies for creating new products, processes, and business models. But one obstacle on the road to digital transformation is placing too much emphasis on technology, and not enough on the types of processes technology enables. What if different lines of business could build their own services and applications—and decision-making was distributed rather than centralized? This report explores the concept of a digital business platform as a way of empowering individual business sectors to act on data in real time. Much innovation in a

digital enterprise will increasingly happen at the edge, whether it involves business users (from marketers to data scientists) or IoT devices. To facilitate the process, your core IT team can provide these sectors with the digital tools they need to innovate quickly. This report explores: Key cultural and organizational changes for developing business capabilities through cross-functional product teams A platform for integrating applications, data sources, business partners, clients, mobile apps, social networks, and IoT devices Creating internal API programs for building innovative edge services in low-code or no-code environments Tools including Integration Platform as a Service, Application Platform as a Service, and Integration Software as a Service The challenge of integrating microservices and serverless architectures Event-driven architectures for processing and reacting to events in real time You'll also learn about a complete pervasive integration solution as a core component of a digital business platform to serve every audience in your organization.

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).

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.

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

[9 Rules for Humans in the Age of Automation](#)

[A Hands-on Approach](#)

[23rd International Computer Symposium, ICS 2018, Yunlin, Taiwan, December 20–22, 2018, Revised Selected Papers](#)

[Hacking Web Intelligence](#)

[Proceedings of ICICCT 2019](#)

[Internet Searches for Vetting, Investigations, and Open-Source Intelligence](#)

[OSINT for the Staffing World!](#)

[Critical Infrastructure Security and Resilience](#)

[From Strategy to Implementation](#)

[Automating Open Source Intelligence](#)

[A Hacker's Guide to Online Intelligence Gathering Tools and Techniques](#)

[Open Source Intelligence and Web Reconnaissance Concepts and Techniques](#)

[Digital Forensics Basics](#)

Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions

A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key Features Employ advanced pentesting techniques with Kali Linux to build highly secured systems Discover various stealth techniques to remain undetected and defeat modern infrastructures Explore red teaming techniques to exploit secured environment Book Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network – directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learn Configure the most effective Kali Linux tools to test infrastructure security Employ stealth to avoid detection in the infrastructure being tested Recognize when stealth attacks are being used against your infrastructure Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network - the end users Who this book is for This third edition of Mastering Kali

Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book.

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.

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.

If you're interested in using social media as an investigative tool, Introduction to Social Media Investigation will show you how! Social networks and social media, like Facebook, Twitter, and Foursquare, are some of the most popular services on the Web, with hundreds of millions of users. The public information that people share on these sites can be valuable for anyone interested in investigating people of interest through open, public sources. Social media as an investigative device is in its infancy and not well understood. This book presents an overview of social media and discusses special skills and techniques to use when conducting investigations. The book features hands-on tutorials and case studies and offers additional data-gathering techniques. Presents an overview of social media sites, information types, privacy policies, and other general issues relevant to investigating individuals online Discusses the special skills and techniques needed when conducting investigations using social media Includes hands-on tutorials and case studies using Facebook, LinkedIn, Twitter, and other social media sites using proven investigative techniques Shows how to gather additional data using advanced techniques such as crowdsourcing, data mining, and network analysis Discover how conservation can be made more effective through strengthening links between science research, policy and practice. This title is also available as Open Access on Cambridge Core.

The 2008 Biosurveillance and Biosecurity Workshop (BioSecure 2008) was built on the success of the two U. S. National Science Foundation-sponsored Biosurveillance Workshops. The inaugural 2006 workshop was hosted by the University of Arizona's NSF BioPortal Center. It attracted more than 35 participants from academic institutions, industry, and public health agencies, and achieved its objective of bringing together infectious disease informatics (IDI) researchers and practitioners to discuss selected topics directly relevant to data sharing and analysis for real-time animal and public health surveillance. The 2007 meeting was held in New Brunswick, New Jersey, co-located with the 2007 IEEE International Conference on Intelligence and Security Informatics, and met with tremendous success. Researchers from a wide range of backgrounds, including biosecurity, epidemiology, statistics, applied mathematics, information systems, computer science and machine learning/data mining, contributed formal papers to the workshop and actively participated in the meeting along with practitioners from both government agencies and industry. More than 65 people attended the one-day workshop, representing major research labs across multiple disciplines, key industry players, and a range of government entities. BioSecure 2008 continued this workshop series aiming to achieve the following objectives: (a) review and examine various informatics approaches for health surveillance and biosecurity from both technological and policy perspectives; and (b) discuss and compare various systems approaches and algorithms of relevance to biosurveillance and biosecurity.

[Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism](#)

[Emerging Research and Opportunities](#)

[Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities](#)

[Open Source Intelligence and Cyber Crime](#)

[Futureproof](#)

[Digital Witness](#)

[On Intelligence](#)

[A Practical Guide Using Windows OS](#)

[Counterterrorism and Open Source Intelligence](#)

[Penetration Testing with Perl](#)

[Open Source Intelligence Investigation](#)

[Activity-Based Intelligence: Principles and Applications](#)

[Inventive Communication and Computational Technologies](#)