[PDF] Intelligence Driven Incident Response Outwitting The Adversary

Getting the books **intelligence driven incident response outwitting the adversary** now is not type of inspiring means. You could not single-handedly going considering books amassing or library or borrowing from your friends to get into them. This is an definitely simple means to specifically get lead by on-line. This online broadcast intelligence driven incident response outwitting the adversary can be one of the options to accompany you later having new time.

It will not waste your time. acknowledge me, the e-book will very manner you extra situation to read. Just invest little epoch to edit this on-line declaration **intelligence driven incident response outwitting the adversary** as well as evaluation them wherever you are now.

Intelligence-Driven Incident Response-Scott J Roberts 2017-08-21 Using a well-conceived incident response plan in the aftermath of an online security breach enables your team to identify attackers and learn how they operate. But, only when you approach incident response with a cyber threat intelligence mindset will you truly understand the value of that information. With this practical guide, you'll learn the fundamentals of intelligence analysis, as well as the best ways to incorporate these techniques into your incident response process. Each method reinforces the other: threat intelligence supports and augments incident response, while incident response generates useful threat intelligence. This book helps incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts understand, implement, and benefit from this relationship. In three parts, this in-depth book includes: The fundamentals: get an introduction to cyber threat intelligence, the intelligence process, the incident-response process, and how they all work together Practical application: walk through the intelligence-driven incident response (IDIR) process using the F3EAD process—Find, Fix Finish, Exploit, Analyze, and Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building

Intelligence-Driven Incident Response-Scott J Roberts 2017-08-21 Using a well-conceived incident response plan in the aftermath of an online security breach enables your team to identify attackers and learn how they operate. But, only when you approach incident response with a cyber threat intelligence mindset will you truly understand the value of that information. With this practical guide, you'll learn the fundamentals of intelligence analysis, as well as the best ways to incorporate these techniques into your incident response process. Each method reinforces the other: threat intelligence supports and augments incident response, while incident response generates useful threat intelligence. This book helps incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts understand, implement, and benefit from this relationship. In three parts, this in-depth book includes: The fundamentals: get an introduction to cyber threat intelligence, the intelligence process, the incident-response process, and how they all work together Practical application: walk through the intelligence-driven incident response (IDIR) process using the F3EAD process—Find, Fix Finish, Exploit, Analyze, and Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building

Intelligence-driven Incident Response-Scott J. Roberts 2016-08-25 Threat intelligence—understanding the who, why, and how of attacks—is most valuable when applied directly to an organization's incident response capability for hunting and investigation. Threat intelligence has become more common and important in recent years. However, many professionals want a better understanding of how to apply this intelligence within their operations and organizations. This book explains the fundamentals of intelligence analysis and the best ways to apply it to your incident response function.

Applied Incident Response-Steve Anson 2020-01-29 Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls

Practical Cyber Intelligence-Wilson Bautista 2018-03-29 Your one stop solution to implement a Cyber Defense Intelligence program in to your organisation. Key Features Intelligence processes and procedures for response mechanisms Master F3EAD to drive processes based on intelligence Threat modeling and intelligent frameworks Case studies and how to go about building intelligent teams Book Description Cyber intelligence is the missing link between your cyber defense operation teams, threat intelligence, and IT operations to provide your organization with a full spectrum of defensive capabilities. This book kicks off with the need for cyber intelligence and why it is required in terms of a defensive framework. Moving forward, the book provides a practical explanation of the F3EAD protocol with the help of examples. Furthermore, we learn how to go about threat models and intelligence products/frameworks and apply them to real-life scenarios. Based on the discussion with the prospective author I would also love to explore the induction of a tool to enhance the marketing feature and functionality of the book. By the end of this book, you will be able to boot up an intelligence program in your organization based on the operation and tactical/strategic spheres of Cyber defense intelligence. What you will learn Learn about the Observe-Orient-Decide-Act (OODA) loop and it's applicability to security Understand tactical view of Active defense concepts and their application in today's threat landscape Get acquainted with an operational view of the F3EAD process to drive decision making within an organization Create a Framework and Capability Maturity Model that integrates inputs and outputs from key functions in an information security organization Understand the idea of communicating with the Potential for Exploitability based on cyber intelligence Who this book is for This book targets incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts; experience in, or knowledge of, security operations, incident responses or investigations is desirable so you can make the most of the subjects presented.

Machine Learning and Security-Clarence Chio 2018-01-26 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

Crafting the InfoSec Playbook-Jeff Bollinger 2015-05-07 Any good attacker will tell you that expensive security monitoring and prevention tools aren’t enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You’ll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone. Written by members of Cisco’s Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture. Learn incident response fundamentals—and the importance of getting back to basics Understand threats you face and what you should be protecting Collect, mine, organize, and analyze as many relevant data sources as possible Build your own playbook of repeatable methods for security monitoring and response Learn how to put your plan into action and keep it running smoothly Select the right monitoring and detection tools for your environment Develop queries to help you sort through data and create valuable reports Know what actions to take during the incident response phase

Cybersecurity Incident Response-Eric C. Thompson 2018-09-20 Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support. Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each phase of incident response are explored in the book. Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You’ll Learn Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team Who This Book Is For Cybersecurity leaders, executives, consultants, and entry-level professionals responsible for executing the incident response plan when something goes wrong

Cyber Intelligence-Driven Risk-Richard O. Moore, III 2020-11-18 Turn cyber intelligence into meaningful business decisions and reduce losses from cyber events Cyber Intelligence-Driven Risk provides a solution to one of the most pressing issues that executives and risk managers face: How can we weave information security into our business decisions to minimize overall business risk? In today's complex digital landscape, business decisions and cyber event responses have implications for information security that high-level actors may be unable to foresee. What we need is a cybersecurity command center capable of delivering, not just data, but concise, meaningful interpretations that allow us to make informed decisions. Building, buying, or outsourcing a CI-DRTM program is the answer. In his work with executives at leading financial organizations and with the U.S. military, author Richard O. Moore III has tested and proven this next-level approach to Intelligence and Risk. This book is a guide to: Building, buying, or outsourcing a cyber intelligence–driven risk program Understanding the functional capabilities needed to sustain the program Using cyber intelligence to support Enterprise Risk Management Reducing loss from cyber events by building new organizational capacities Supporting mergers and acquisitions with predictive analytics Each function of a well-designed cyber intelligence-driven risk program can support informed business decisions in the era of increased complexity and emergent cyber threats.

Effective Threat Intelligence-James Dietle 2016-06-23 You already have the tools to make a threat intel program! With the growing number of threats against companies, threat intelligence is becoming a business essential. This book will explore steps facts and myths on how to effectively formalize and improve the intel program at your company by:* Separating good and bad intelligence* Creating a threat intelligence maturity model* Quantifying threat risk to your organization* How to build and structure a threat intel team* Ways to build intel talent from withinWith a wider array of information freely available to the public you do not want to be caught without an understanding of the threats to your company. Explore some ideas to help formalize the efforts to create a safer environment for employees and clients.

Security Operations Center-Joseph Muniz 2015-11-02 Security Operations Center Building, Operating, and Maintaining Your SOC The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC) Security Operations Center is the complete guide to building, operating, and managing Security Operations Centers in any environment. Drawing on experience with hundreds of customers ranging from Fortune 500 enterprises to large military organizations, three leading experts thoroughly review each SOC model, including virtual SOCs. You’ll learn how to select the right strategic option for your organization, and then plan and execute the strategy you’ve chosen. Security Operations Center walks you through every phase required to establish and run an effective SOC, including all significant people, process, and technology capabilities. The authors assess SOC technologies, strategy, infrastructure, governance, planning, implementation, and more. They take a holistic approach considering various commercial and open-source tools found in modern SOCs. This best-practice guide is written for anybody interested in learning how to develop, manage, or improve a SOC. A background in network security, management, and operations will be helpful but is not required. It is also an indispensable resource for anyone preparing for the Cisco SCYBER exam. · Review high-level issues, such as vulnerability and risk management, threat intelligence, digital investigation, and data collection/analysis · Understand the technical components of a modern SOC · Assess the current state of your SOC and identify areas of improvement · Plan SOC strategy, mission, functions, and services · Design and build out SOC infrastructure, from facilities and networks to systems, storage, and physical security · Collect and successfully analyze security data · Establish an effective vulnerability management practice · Organize incident response teams and measure their performance · Define an optimal governance and staffing model · Develop a practical SOC handbook that people can actually use · Prepare SOC to go live, with comprehensive transition plans · React quickly and collaboratively to security incidents · Implement best practice security operations, including continuous enhancement and improvement

Threat Modeling-Adam Shostack 2014-02-12 The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

The Practice of Network Security Monitoring-Richard Bejtlich 2013-07-15 Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: –Determine where to deploy NSM platforms, and size them for the monitored networks –Deploy stand-alone or distributed NSM installations –Use command line and graphical packet analysis tools, and NSM consoles –Interpret network evidence from server-side and client-side intrusions –Integrate threat intelligence into NSM software to identify sophisticated adversaries There’s no foolproof way to keep attackers out of your network. But when they get in, you’ll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Investigating the Cyber Breach-Joseph Muniz 2018-01-31 Investigating the Cyber Breach The Digital Forensics Guide for the Network Engineer · Understand the realities of cybercrime and today’s attacks · Build a digital forensics lab to test tools and methods, and gain expertise · Take the right actions as soon as you discover a breach · Determine the full scope of an investigation and the role you’ll play · Properly collect, document, and preserve evidence and data · Collect and analyze data from PCs, Macs, IoT devices, and other endpoints · Use packet logs, NetFlow, and scanning to build timelines, understand network activity, and collect evidence · Analyze iOS and Android devices, and understand encryption-related obstacles to investigation · Investigate and trace email, and identify fraud or abuse · Use social media to investigate individuals or online identities · Gather, extract, and analyze breach data with Cisco tools and techniques · Walk through common breaches and responses from start to finish · Choose the right tool for each task, and explore alternatives that might also be helpful The professional’s go-to digital forensics resource for countering attacks right now Today, cybersecurity and networking professionals know they can’t possibly prevent every breach, but they can substantially reduce risk by quickly identifying and blocking breaches as they occur. Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer is the first comprehensive guide to doing just that. Writing for working professionals, senior cybersecurity experts Joseph Muniz and Aamir Lakhani present up-to-the-minute techniques for hunting attackers, following their movements within networks, halting exfiltration of data and intellectual property, and collecting evidence for investigation and prosecution. You’ll learn how to make the most of today’s best open source and Cisco tools for cloning, data analytics, network and endpoint breach detection, case management, monitoring, analysis, and more. Unlike digital forensics books focused primarily on post-attack evidence gathering, this one offers complete coverage of tracking threats, improving intelligence, rooting out dormant malware, and responding effectively to breaches underway right now. This book is part of the Networking Technology: Security Series from Cisco Press®, which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

Mindstorms-Seymour A. Papert 2020-10-06 In this revolutionary book, a renowned computer scientist explains the importance of teaching children the basics of computing and how it can prepare them to succeed in the ever-evolving tech world. Computers have completely changed the way we teach children. We have Mindstorms to thank for that. In this book, pioneering computer scientist Seymour Papert uses the invention of LOGO, the first child-friendly programming language, to make the case for the value of teaching children with computers. Papert argues that children are more than capable of mastering computers, and that teaching computational processes like de-bugging in the classroom can change the way we learn everything else. He also shows that schools saturated with technology can actually improve socialization and interaction among students and between students and teachers. Technology changes every day, but the basic ways that computers can help us learn remain. For thousands of teachers and parents who have sought creative ways to help children learn with computers, Mindstorms is their bible.

Simulation for Applied Graph Theory Using Visual C++-Shaharuddin Salleh 2016-08-19 The tool for visualization is Microsoft Visual C++. This popular software has the standard C++ combined with the Microsoft Foundation Classes (MFC) libraries for Windows visualization. This book explains how to create a graph interactively, solve problems in graph theory with minimum number of C++ codes, and provide friendly interfaces that makes learning the topics an interesting one. Each topic in the book comes with working Visual C++ codes which can easily be adapted as solutions to various problems in science and engineering.

Attribution of Advanced Persistent Threats-Timo Steffens 2020-07-20 An increasing number of countries develop capabilities for cyber-espionage and sabotage. The sheer number of reported network compromises suggests that some of these countries view cyber-means as integral and well-established elements of their strategical toolbox. At the same time the relevance of such attacks for society and politics is also increasing. Digital means were used to influence the US presidential election in 2016, repeatedly led to power outages in Ukraine, and caused economic losses of hundreds of millions of dollars with a malfunctioning ransomware. In all these cases the question who was behind the attacks is not only relevant from a legal perspective, but also has a political and social dimension. Attribution is the process of tracking and identifying the actors behind these cyber-attacks. Often it is considered an art, not a science. This book systematically analyses how hackers operate, which mistakes they make, and which traces they leave behind. Using examples from real cases the author explains the analytic methods used to ascertain the origin of Advanced Persistent Threats.

CUCKOO'S EGG-Clifford Stoll 2012-05-23 Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Building a Home Security System with Arduino-Jorge R. Castro 2015-09-01 Design, build and maintain a home security system with Arduino Uno About This Book Learn what a security system is, how it works and create one for yourself Develop a security system by setting up security cameras and motion detector systems Manage and analyze all the data collected by the sensors from the security system, using a graphical application Who This Book Is For This book is for novice programmers and hobbyists who want to understand how Arduino can be used to program a home security system as well as to those who want to delve deeper into the world of Arduino. What You Will Learn Run cables and electricity to support home security infrastructure Connect Arduino to your programming environment Learn to interact with output devices – alarms, locks, shutters Understand different parts of electronics circuit (MOSFET, resistor, capacitor) Integrate home monitoring and security notifications with monitoring systems Use logical level shifter with

Arduino to send and receive data to and from Raspberry PI In Detail Arduino is an open source micro-controller built on a single circuit board that is capable of receiving sensory input from the environment and controlling interactive physical objects. It is also a development environment that allows the writing of software to the board, and is programmed in the Arduino programming language. It is used for a variety of different purposes and projects, from simple projects such as building a thermostat, to more advanced ones such as robotics, web servers, seismographs, home security systems and synthesizers. This book will demonstrate how the Arduino can be used to develop a highly connected home security system by mobilizing a network of sensors which can feed alerts back to an Arduino when alarms are triggered. You will know the current state of security systems, well supported by the designs that fit best for your environment. Also, we will see some current technologies such as NFC, Wi-Fi and Bluetooth, and will finally create a complete web interface that will allow us to remotely manage our system, and even send daily bulletins with the summary of activity. Towards the end, we'll develop a wireless home security system by setting up security cameras and motion detectors (door and gate trips, temperature sensors). We will then set up a centralized remote access hub (powered by the Arduino) that allows sensors to connect to the wireless home network that can be viewed and interacted by the user. Style and approach A step-by-step guide with numerous examples focusing on providing the practical skills required to build home security applications using Arduino.

Defensive Security Handbook-Lee Brotherston 2017-04-03 Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don’t have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring

Intelligence Analysis: How to Think in Complex Environments-Wayne Michael Hall 2009-12-22 This book offers a vast conceptual and theoretical exploration of the ways intelligence analysis must change in order to succeed against today's most dangerous combatants and most complex irregular theatres of conflict. • Includes quotations from a wide range of acclaimed thinkers • Offers an extensive bibliography of works cited and resources for further reading • Presents a comprehensive index

The Art of Cyber Leadership-Matt Doan 2018-11-16

OS X Incident Response-Jaron Bradley 2016-05-07 OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset. Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations. Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones. Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately. For online source codes, please visit: https://github.com/jbradley89/osx_incident_response_scripting_and_analysis Focuses exclusively on OS X attacks, incident response, and forensics Provides the technical details of OS X so you can find artifacts that might be missed using automated tools Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

Machine Learning Projects for .NET Developers-Mathias Brandewinder 2015-07-09 Machine Learning Projects for .NET Developers shows you how to build smarter .NET applications that learn from data, using simple algorithms and techniques that can be applied to a wide range of real-world problems. You'll code each project in the familiar setting of Visual Studio, while the machine learning logic uses F#, a language ideally suited to machine learning applications in .NET. If you're new to F#, this book will give you everything you need to get started. If you're already familiar with F#, this is your chance to put the language into action in an exciting new context. In a series of fascinating projects, you'll learn how to: Build an optical character recognition (OCR) system from scratch Code a spam filter that learns by example Use F#'s powerful type providers to interface with external resources (in this case, data analysis tools from the R programming language) Transform your data into informative features, and use them to make accurate predictions Find patterns in data when you don't know what you're looking for Predict numerical values using regression models Implement an intelligent game that learns how to play from experience Along the way, you'll learn fundamental ideas that can be applied in all kinds of real-world contexts and industries, from advertising to finance, medicine, and scientific research. While some machine learning algorithms use fairly advanced mathematics, this book focuses on simple but effective approaches. If you enjoy hacking code and data, this book is for you.

Methland-Nick Reding 2010-06-03 Traces the efforts of a small Iowa community to counter the pervasiveness of crystal methamphetamine, in an account that offers insight into the drug's appeal while chronicling the author's numerous visits with the town's doctor, the local prosecutor and a long-time addict. Reprint. A best-selling book.

The Cyber Intelligence Handbook-David M Cooney Jr 2019-07-26 Seize the initiative from cyber-threat actors by applying cyber intelligence to create threat-driven cybersecurity operations! Written by an intelligence professional with 40 years of experience applying intelligence to counter threats from a wide range of determined adversaries, this book provides common sense practices for establishing and growing responsive cyber intelligence capabilities customized to organization needs, regardless of size or industry. Readers will learn: -What cyber intelligence is and how to apply it to deter, detect, and defeat malicious cyber-threat actors targeting your networks and data;-How to characterize threats and threat actors with precision to enable all relevant stakeholders to contribute to desired security outcomes;-A three-step planning approach that allows cyber intelligence customers to define and prioritize their needs;-How to construct a simplified cyber intelligence process that distills decades of national-level intelligence community doctrine into a sets of clearly defined, mutually supporting actions that will produce repeatable and measureable results from the outset;-How to employ advanced analytic frameworks to apply intelligence as an operational function that can inform security design and execution to complicate actions for would be attackers.

Hands-On Red Team Tactics-Himanshu Sharma 2018-09-28 Your one-stop guide to learning and implementing Red Team tactics effectively Key Features Target a complex enterprise environment in a Red Team activity Detect threats and respond to them with a real-world cyber-attack simulation Explore advanced penetration testing tools and techniques Book Description Red Teaming is used to enhance security by performing simulated attacks on an organization in order to detect network and system vulnerabilities. Hands-On Red Team Tactics starts with an overview of pentesting and Red Teaming, before giving you an introduction to few of the latest pentesting tools. We will then move on to exploring Metasploit and getting to grips with Armitage. Once you have studied the fundamentals, you will learn how to use Cobalt Strike and how to set up its team server. The book introduces some common lesser known techniques for pivoting and how to pivot over SSH, before using Cobalt Strike to pivot. This comprehensive guide demonstrates advanced methods of post-exploitation using Cobalt Strike and introduces you to Command and Control (C2) servers and redirectors. All this will help you achieve persistence using beacons and data exfiltration, and will also give you the chance to run through the methodology to use Red Team activity tools such as Empire during a Red Team activity on Active Directory and Domain Controller. In addition to this, you will explore maintaining persistent access, staying untraceable, and getting reverse connections over different C2 covert channels. By the end of this book, you will have learned about advanced penetration testing tools, techniques to get reverse shells over encrypted channels, and processes for post-exploitation. What you will learn Get started with red team engagements using lesser-known methods Explore intermediate and advanced levels of post-exploitation techniques Get acquainted with all the tools and frameworks included in the Metasploit framework Discover the art of getting stealthy access to systems via Red Teaming Understand the concept of redirectors to add further anonymity to your C2 Get to grips with different uncommon techniques for data exfiltration Who this book is for Hands-On Red Team Tactics is for you if you are an IT professional, pentester, security consultant, or ethical hacker interested in the IT security domain and wants to go beyond Penetration Testing. Prior knowledge of penetration testing is beneficial.

Cyber Threat Intelligence-Ali Dehghantanha 2018-04-27 This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

Cyberjutsu-Ben McCarty 2021 "Teaches ancient approaches to modern information security issues based on authentic, formerly classified ninja scrolls"--

Outwitting the Hun-Pat O'Brien 1918

Blue Team Handbook-Don Murdoch 2014-08-03 Updated, Expanded, and released to print on 10/5/14! Complete details below! Two new sections, five protocol header illustrations, improved formatting, and other corrections. The Blue Team Handbook is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics. The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way. Version 2.0 updates: - *** A new section on Database incident response was added. - *** A new section on Chain of Custody was added. - *** Matt Baxter's superbly formatted protocol headers were added! - Table headers bolded. - Table format slightly revised throughout book to improve left column readability. - Several sentences updated and expanded for readability and completeness. - A few spelling errors were corrected. - Several sites added to the Web References section. - Illustrations reformatted for better fit on the page. - An index was added. - Attribution for some content made more clear (footnotes, expanded source citing) - Content expanded a total of 20 pages

CompTIA CySA+ Practice Tests-Mike Chapple 2020-09-01 Efficiently prepare yourself for the demanding CompTIA CySA+ exam CompTIA CySA+ Practice Tests: Exam CS0-002, 2nd Edition offers readers the fastest and best way to prepare for the CompTIA Cybersecurity Analyst exam. With five unique chapter tests and two additional practice exams for a total of 1000 practice questions, this book covers topics including: Threat and Vulnerability Management Software and Systems Security Security Operations and Monitoring Incident Response Compliance and Assessment The new edition of CompTIA CySA+ Practice Tests is designed to equip the reader to tackle the qualification test for one of the most sought-after and in-demand certifications in the information technology field today. The authors are seasoned cybersecurity professionals and leaders who guide readers through the broad spectrum of security concepts and technologies they will be required to master before they can achieve success on the CompTIA CySA exam. The book also tests and develops the critical thinking skills and judgment the reader will need to demonstrate on the exam.

The Freedmen's Book-Lydia Maria Child 1866 SpanPublished in 1865 and edited by abolitionist L. Maria Child, The Freedmens Book was intended to be used to teach recently freed African Americans to read and to provide them with inspiration. Thirsting for education, Freedmen were eagerly enrolling in any schools that would accept them. Child saw a need for texts and provided one of collected stories and poems written by former slaves and noted abolitionists, herself included./span

The Idea Factory-Jon Gertner 2013 Highlights achievements of Bell Labs as a leading innovator, exploring the role of its highly educated employees in developing new technologies while considering the qualities of companies where innovation and development are most successful.

The Martian-Andy Weir 2021-03-30 #1 NEW YORK TIMES BESTSELLER * "Brilliant . . . a celebration of human ingenuity [and] the purest example of real-science sci-fi for many years . . . utterly compelling."--The Wall Street Journal The inspiration for the major motion picture Six days ago, astronaut Mark Watney became one of the first people to walk on Mars. Now, he's sure he'll be the first person to die there. After a dust storm nearly kills him and forces his crew to evacuate while thinking him dead, Mark finds himself stranded and completely alone with no way to even signal Earth that he's alive--and even if he could get word out, his supplies would be gone long before a rescue could arrive. Chances are, though, he won't have time to starve to death. The damaged machinery, unforgiving environment, or plain-old "human error" are much more likely to kill him first. But Mark isn't ready to give up yet. Drawing on his ingenuity, his engineering skills--and a relentless, dogged refusal to quit--he steadfastly confronts one seemingly insurmountable obstacle after the next. Will his resourcefulness be enough to overcome the impossible odds against him? NAMED ONE OF PASTE'S BEST NOVELS OF THE DECADE "A hugely entertaining novel [that] reads like a rocket ship afire . . . Weir has fashioned in Mark Watney one of the most appealing, funny, and resourceful characters in recent fiction."--Chicago Tribune "As gripping as they come . . . You'll be rooting for Watney the whole way, groaning at every setback and laughing at his pitchblack humor. Utterly nail-biting and memorable."--Financial Times

Unbroken-Laura Hillenbrand 2014-07-29 Relates the story of a U.S. airman who survived when his bomber crashed into the sea during World War II, spent forty-seven days adrift in the ocean before being rescued by the Japanese Navy, and was held as a prisoner until the end of the war.

Day Of Deceit-Robert Stinnett 2001-05-08 Using previously unreleased documents, the author reveals new evidence that FDR knew the attack on Pearl Harbor was coming and did nothing to prevent it.

Hawaii's Story-Liliuokalani (Queen of Hawaii) 1898

Red Team Development and Operations-James Tubberville 2020-01-20 This book is the culmination of years of experience in the information technology and cybersecurity field. Components of this book have existed as rough notes, ideas, informal and formal processes developed and adopted by the authors as they led and executed red team engagements over many years. The concepts described in this book have been used to successfully plan, deliver, and perform professional red team engagements of all sizes and complexities. Some of these concepts were loosely documented and integrated into red team management processes, and much was kept as tribal knowledge. One of the first formal attempts to capture this information was the SANS SEC564 Red Team Operation and Threat Emulation course. This first effort was an attempt to document these ideas in a format usable by others. The authors have moved beyond SANS training and use this book to detail red team operations in a practical guide. The authors' goal is to provide practical guidance to aid in the management and execution of professional red teams. The term 'Red Team' is often confused in the cybersecurity space. The terms roots are based on military concepts that have slowly made their way into the commercial space. Numerous interpretations directly affect the scope and quality of today's security engagements. This confusion has created unnecessary difficulty as organizations attempt to measure threats from the results of quality security assessments. You quickly understand the complexity of red teaming by performing a quick google search for the definition, or better yet, search through the numerous interpretations and opinions posted by security professionals on Twitter. This book was written to provide a practical solution to address this confusion. The Red Team concept requires a unique approach different from other security tests. It relies heavily on well-defined TTPs critical to the successful simulation of realistic threat and adversary techniques. Proper Red Team results are much more than just a list of flaws identified during other security tests. They provide a deeper understanding of how an organization would perform against an actual threat and determine where a security operation's strengths and weaknesses exist.Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve defenses is extremely valuable. Organizations spend a great deal of time and money on the security of their systems. It is critical to have professionals who understand the threat and can effectively and efficiently operate their tools and techniques safely and professionally. This book will provide you with the real-world guidance needed to manage and operate a professional Red Team, conduct quality engagements, understand the role a Red Team plays in security operations. You will explore Red Team concepts in-depth, gain an understanding of the fundamentals of threat emulation, and understand tools needed you reinforce your organization's security posture.

RESTful PHP Web Services-Samisa Abeysinghe 2008-10-30 Learn the basic architectural concepts and step through examples of consuming and creating RESTful web services in PHP.