Learning Malware Analysis Explore The Concepts To

Thank you very much for reading **learning malware analysis explore the concepts to**. As you may know, people have search numerous times for their favorite books like this learning malware analysis explore the concepts to, but end up in infectious downloads.
Rather than reading a good book with a cup of coffee in the afternoon, instead they cope with some malicious bugs inside their laptop.

learning malware analysis explore the concepts to is available in our digital library an online access to it is set as public so you can download it instantly.
Our book servers spans in multiple countries, allowing you to get the most less latency time to download any of our books like this one.
Merely said, the learning malware analysis explore the concepts to is universally compatible with any devices to read

JavaScript Security Y.E Liang 2014-11-22 This book is for JavaScript developers having basic web development knowledge and also for those who want to explore the security issues that arise from the use of JavaScript. Prior knowledge of how JavaScript is used, such as for DOM manipulation or to perform Ajax operations, is assumed.

Malware Forensics Field Guide for Windows Systems Cameron H. Malin 2012-06-13 Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treaterous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, Malware Forensics Field Guide for Windows Systems is a "tool" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code

Mastering Malware Analysis Alexey Kleymenov 2019-06-06 Master malware analysis to protect your systems from getting infected Key FeaturesSet up and model solutions, investigate malware, and prevent it from occurring in futureLearn core concepts of dynamic malware analysis, memory forensics, decryption, and much moreA practical guide to developing innovative solutions to numerous malware incidentsBook Description With the ever-growing proliferation of technology, the risk of encountering malicious code or malware has also increased. Malware analysis has become one of the most trending topics in businesses in recent years due to multiple prominent ransomware attacks. Mastering Malware Analysis explains the universal patterns behind different malicious software types and how to analyze them using a variety of approaches. You will learn how to examine malware code and determine the damage it can possibly cause to your systems to ensure that it won't propagate any further. Moving forward, you will cover all aspects of malware analysis for the Windows platform in detail. Next, you will get to grips with obfuscation and anti-disassembly, anti-debugging, as well as anti-virtual machine techniques. This

book will help you deal with modern cross-platform malware. Throughout the course of this book, you will explore real-world examples of static and dynamic malware analysis, unpacking and decrypting, and rootkit detection. Finally, this book will help you strengthen your defenses and prevent malware breaches for IoT devices and mobile platforms. By the end of this book, you will have learned to effectively analyze, investigate, and build innovative solutions to handle any malware incidents. What you will learnExplore widely used assembly languages to strengthen your reverse-engineering skillsMaster different executable file formats, programming languages, and relevant APIs used by attackersPerform static and dynamic analysis for multiple platforms and file typesGet to grips with handling sophisticated malware casesUnderstand real advanced attacks, covering all stages from infiltration to hacking the systemLearn to bypass anti-reverse engineering techniquesWho this book is for If you are an IT security administrator, forensic analyst, or malware researcher looking to secure against malicious software or investigate malicious code, this book is for you. Prior programming experience and a fair understanding of malware attacks and investigation is expected.

Malware Analyst's Cookbook and DVD Michael Ligh 2010-09-29 A computer forensics "how-to" for fighting malicious code andanalyzing incidents With our ever-increasing reliance on computers comes anever-growing risk of malware. Security professionals will findplenty of solutions in this book to the problems posed by viruses,Trojan horses, worms, spyware, rootkits, adware, and other invasivesoftware. Written by well-known malware experts, this guide revealssolutions to numerous problems and includes a DVD of customprograms and tools that illustrate the concepts, enhancing yourskills. Security professionals face a constant battle against maliciousoftware; this practical manual will improve your analyticalcapabilities and provide dozens of valuable and innovativesolutions Covers classifying malware, packing and unpacking, dynamicmalware analysis, decoding and decrypting, rootkit detection,memory forensics, open source malware research, and much more Includes generous amounts of source code in C, Python, and Perlto extend your favorite tools or build new ones, and customprograms on the DVD to demonstrate the solutions Malware Analyst's Cookbook is indispensible to ITsecurity administrators, incident responders, forensic analysts,and malware researchers.

Practical Mobile Forensics Satish Bommisetty 2014-07-21 The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book.

Ransomware Allan Liska 2016-11-21 The biggest online threat to businesses and consumers today is ransomware, a category of malware that can encrypt your computer files until you pay a ransom to unlock them. With this practical book, you'll learn how easily ransomware infects your system and what steps you can take to stop the attack before it sets foot in the network. Security experts Allan Liska and Timothy Gallo explain how the success of these attacks has spawned not only several variants of ransomware, but also a litany of ever-changing ways they're delivered to targets. You'll learn pragmatic methods for responding quickly to a ransomware attack, as well as how to protect yourself

from becoming infected in the first place. Learn how ransomware enters your system and encrypts your files Understand why ransomware use has grown, especially in recent years Examine the organizations behind ransomware and the victims they target Learn how wannabe hackers use Ransomware as a Service (RaaS) to launch campaigns Understand how ransom is paid—and the pros and cons of paying Use methods to protect your organization's workstations and servers

Windows Malware Analysis Essentials Victor Marak 2015-09-01 Master the fundamentals of malware analysis for the Windows platform and enhance your anti-malware skill set About This Book Set the baseline towards performing malware analysis on the Windows platform and how to use the tools required to deal with malware Understand how to decipher x86 assembly code from source code inside your favourite development environment A step-by-step based guide that reveals malware analysis from an industry insider and demystifies the process Who This Book Is For This book is best for someone who has prior experience with reverse engineering Windows executables and wants to specialize in malware analysis. The book presents the malware analysis thought process using a show-and-tell approach, and the examples included will give any analyst confidence in how to approach this task on their own the next time around. What You Will Learn Use the positional number system for clear conception of Boolean algebra, that applies to malware research purposes Get introduced to static and dynamic analysis methodologies and build your own malware lab Analyse destructive malware samples from the real world (ITW) from fingerprinting and static/dynamic analysis to the final debrief Understand different modes of linking and how to compile your own libraries from assembly code and integrate the codein your final program Get to know about the various emulators, debuggers and their features, and sandboxes and set them up effectively depending on the required scenario Deal with other malware vectors such as pdf and MS-Office based malware as well as scripts and shellcode In Detail Windows OS is the most used operating system in the world and hence is targeted by malware writers. There are strong ramifications if things go awry. Things will go wrong if they can, and hence we see a salvo of attacks that have continued to disrupt the normal scheme of things in our day to day lives. This book will guide you on how to use essential tools such as debuggers, disassemblers, and sandboxes to dissect malware samples. It will expose your innards and then build a report of their indicators of compromise along with detection rule sets that will enable you to help contain the outbreak when faced with such a situation. We will start with the basics of computing fundamentals such as number systems and Boolean algebra. Further, you'll learn about x86 assembly programming and its integration with high level languages such as C++.You'll understand how to decipher disassembly code obtained from the compiled source code and map it back to its original design goals. By delving into end to end analysis with real-world malware samples to solidify your understanding, you'll sharpen your technique of handling destructive malware binaries and vector mechanisms. You will also be encouraged to consider analysis lab safety measures so that there is no infection in the process. Finally, we'll have a rounded tour of various emulations, sandboxing, and debugging options so that you know what is at your disposal when you need a specific kind of weapon in order to nullify the malware. Style and approach An easy to follow, hands-on guide with descriptions and screenshots that will help you execute effective malicious software investigations and conjure up solutions creatively and confidently.

Digital Forensics Basics Nihad A. Hassan 2019-02-25 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 investigationsGather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10-specific feature forensicsUtilize 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

Learning Android Forensics Oleg Skulkin 2018-12-28 A comprehensive guide to Android forensics, from setting up the workstation to analyzing key artifacts Key FeaturesGet up and running with modern mobile forensic strategies and techniquesAnalyze the most popular Android applications using free and open source forensic toolsLearn malware detection and analysis techniques to investigate mobile cybersecurity incidentsBook Description Many forensic examiners rely on commercial, push-button tools to retrieve and analyze data, even though there is no tool that does either of these jobs perfectly. Learning Android Forensics will introduce you to the most up-to-date Android platform and its architecture, and provide a high-level overview of what Android forensics entails. You will understand how data is stored on Android devices and how to set up a digital forensic examination environment. As you make your way through the chapters, you will work through various physical and logical techniques to extract data from devices in order to obtain forensic evidence. You will also learn how to recover deleted data and forensically analyze application data with the help of various open source and commercial tools. In the concluding chapters, you will explore malware analysis so that you'll be able to investigate cybersecurity incidents involving Android malware. By the end of this book, you will have a complete understanding of the Android forensic process, you will have explored open source and commercial forensic tools, and will have basic skills of Android malware identification and analysis. What you will learnUnderstand Android OS and architectureSet up a forensics environment for Android analysisPerform logical and physical data extractionsLearn to recover deleted dataExplore how to analyze application dataIdentify malware on Android devicesAnalyze Android malwareWho this book is for If you are a forensic analyst or an information security professional wanting to develop your knowledge of Android forensics, then this is the book for you. Some basic knowledge of the Android mobile platform is expected.

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.

Mobile Malware Attacks and Defense Ken Dunham 2008-11-12 Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone. Examining code in past, current, and future risks, protect your banking, auctioning, and other activities performed on mobile devices. * Visual Payloads View attacks as visible to the end user, including notation of variants. * Timeline of Mobile Hoaxes and Threats Understand the history of major attacks and horizon for emerging threates. * Overview of Mobile Malware Families Identify and understand groups of mobile malicious code and their variations. * Taxonomy of Mobile Malware Bring order to known samples based on infection, distribution, and payload strategies. * Phishing, SMishing, and Vishing Attacks Detect and mitigate phone-based phishing (vishing) and SMS phishing (SMishing) techniques. * Operating System and Device Vulnerabilities Analyze unique OS security issues and examine offensive mobile device threats. * Analyze Mobile Malware Design a sandbox for dynamic software analysis and use MobileSandbox to analyze mobile malware. * Forensic Analysis of Mobile Malware Conduct forensic analysis of mobile devices and learn key differences in mobile forensics. * Debugging and Disassembling Mobile Malware Use IDA and other tools to reverse-engineer samples of malicious code for analysis. * Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats

Essential Cybersecurity Science Josiah Dykstra 2015-12-08 If you're involved in cybersecurity as a software developer, forensic investigator, or network administrator, this practical guide shows you how to apply the scientific method when assessing techniques for protecting your information systems. You'll learn how to conduct scientific experiments on everyday tools and procedures, whether you're evaluating corporate security systems, testing your own security product, or looking for bugs in a mobile game. Once author Josiah Dykstra gets you up to speed on the scientific method, he helps you focus on standalone, domain-specific topics, such as cryptography, malware analysis, and system security engineering. The latter chapters include practical case studies that demonstrate how to use available tools to conduct domain-specific scientific experiments. Learn the steps necessary to conduct scientific experiments in cybersecurity Explore fuzzing to test how your software handles various inputs Measure the performance of the Snort intrusion detection system Locate malicious "needles in a haystack" in your network and IT environment Evaluate cryptography design and application in IoT products Conduct an experiment to identify relationships between similar malware binaries Understand system-level security requirements for enterprise networks and web services

Cybersecurity Attacks – Red Team Strategies Johann Rehberger 2020-03-31 Develop your red team skills by learning essential foundational tactics, techniques, and procedures, and boost the overall security posture of your organization by leveraging the homefield advantage Key Features Build, manage, and measure an offensive red team program Leverage the homefield advantage to stay ahead of your adversaries Understand core adversarial tactics and techniques, and protect pentesters and pentesting assets Book Description It's now more important than ever for organizations to be ready to detect and respond to security events and breaches. Preventive measures alone are not enough for dealing with adversaries. A well-rounded prevention, detection, and response program is required. This book will guide you through the stages of building a red team program, including strategies and homefield advantage opportunities to boost security. The book starts by guiding you through establishing, managing, and measuring a red team program, including effective ways for sharing results and findings to raise awareness. Gradually, you'll learn about progressive operations such as cryptocurrency mining, focused privacy testing, targeting telemetry, and even blue team tooling. Later, you'll discover knowledge graphs and how to build them, then become well-versed with basic to advanced techniques related to hunting for credentials, and learn to automate Microsoft Office and browsers to your advantage. Finally, you'll get to grips with protecting assets using decoys, auditing, and alerting with examples for major operating systems. By the end of this book, you'll have learned how to build, manage, and measure a red team program effectively and be well-versed with the fundamental operational techniques required to enhance your existing skills. What you will learn Understand the risks associated with security breaches Implement strategies for building an effective penetration testing team Map out the homefield using knowledge graphs Hunt credentials using indexing and other practical techniques Gain blue team tooling insights to enhance your red team skills Communicate results and influence decision makers with appropriate data Who this book is for This is one of the few detailed cybersecurity books for penetration testers, cybersecurity analysts, security leaders and strategists, as well as red team members and chief information security officers (CISOs) looking to secure their organizations from adversaries. The program management part of this book will also be useful for beginners in the cybersecurity domain. To get the most out of this book, some penetration testing experience,

and software engineering and debugging skills are necessary.

Security Warrior Cyrus Peikari 2004-01-12 When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm.What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antiforensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle.Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability.Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands.

Windows Forensic Analysis Toolkit Harlan Carvey 2014-03-11 Harlan Carvey has updated Windows Forensic Analysis Toolkit, now in its fourth edition, to cover Windows 8 systems. The primary focus of this edition is on analyzing Windows 8 systems and processes using free and open-source tools. The book covers live response, file analysis, malware detection, timeline, and much more. Harlan Carvey presents real-life experiences from the trenches, making the material realistic and showing the why behind the how. The companion and toolkit materials are hosted online. This material consists of electronic printable checklists, cheat sheets, free custom tools, and walk-through demos. This edition complements Windows Forensic Analysis Toolkit, Second Edition, which focuses primarily on XP, and Windows Forensic Analysis Toolkit, Third Edition, which focuses primarily on Windows 7. This new fourth edition provides expanded coverage of many topics beyond Windows 8 as well, including new cradle-to-grave case examples, USB device analysis, hacking and intrusion cases, and "how would I do this" from Harlan's personal case files and questions he has received from readers. The fourth edition also includes an all-new chapter on reporting. Complete coverage and examples of Windows 8 systems Contains lessons from the field, case studies, and war stories Companion online toolkit material, including electronic printable checklists, cheat sheets, custom tools, and walk-throughs

Network Security and Cryptography Sarhan M. Musa 2018-03-20 Network Security and Cryptography introduces the basic concepts in computer networks and the latest trends and technologies in cryptography and network security. The book is a definitive guide to the principles and techniques of cryptography and network security, and introduces basic concepts in computer networks such as classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, and Internet security. It features the latest material on emerging technologies, related to IoT, cloud computing, SCADA, blockchain, smart grid, big data analytics, and more. Primarily intended as a textbook for courses in computer science and electronics & communication, the book also

serves as a basic reference and refresher for professionals in these areas. FEATURES: • Includes the latest material on emerging technologies, related to IoT, cloud computing, smart grid, big data analytics, blockchain, and more • Features separate chapters on the mathematics related to network security and cryptography • Introduces basic concepts in computer networks including classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, Internet security services, and system security • Includes end of chapter review questions

Malware Analysis Using Artificial Intelligence and Deep Learning Mark Stamp 2020-12-20 This book is focused on the use of deep learning (DL) and artificial intelligence (AI) as tools to advance the fields of malware detection and analysis. The individual chapters of the book deal with a wide variety of state-of-the-art AI and DL techniques, which are applied to a number of challenging malware-related problems. DL and AI based approaches to malware detection and analysis are largely data driven and hence minimal expert domain knowledge of malware is needed. This book fills a gap between the emerging fields of DL/AI and malware analysis. It covers a broad range of modern and practical DL and AI techniques, including frameworks and development tools enabling the audience to innovate with cutting-edge research advancements in a multitude of malware (and closely related) use cases.

Mastering Malware Analysis Alexey Kleymenov 2019-06-06 Master malware analysis to protect your systems from getting infected Key Features Set up and model solutions, investigate malware, and prevent it from occurring in future Learn core concepts of dynamic malware analysis, memory forensics, decryption, and much more A practical guide to developing innovative solutions to numerous malware incidents Book Description With the ever-growing proliferation of technology, the risk of encountering malicious code or malware has also increased. Malware analysis has become one of the most trending topics in businesses in recent years due to multiple prominent ransomware attacks. Mastering Malware Analysis explains the universal patterns behind different malicious software types and how to analyze them using a variety of approaches. You will learn how to examine malware code and determine the damage it can possibly cause to your systems to ensure that it won't propagate any further. Moving forward, you will cover all aspects of malware analysis for the Windows platform in detail. Next, you will get to grips with obfuscation and anti-disassembly, anti-debugging, as well as anti-virtual machine techniques. This book will help you deal with modern cross-platform malware. Throughout the course of this book, you will explore real-world examples of static and dynamic malware analysis, unpacking and decrypting, and rootkit detection. Finally, this book will help you strengthen your defenses and prevent malware breaches for IoT devices and mobile platforms. By the end of this book, you will have learned to effectively analyze, investigate, and build innovative solutions to handle any malware incidents. What you will learn Explore widely used assembly languages to strengthen your reverse-engineering skills Master different executable file formats, programming languages, and relevant APIs used by attackers Perform static and dynamic analysis for multiple platforms and file types Get to grips with handling sophisticated malware cases Understand real advanced attacks, covering all stages from infiltration to hacking the system Learn to bypass anti-reverse engineering techniques Who this book is for If you are an IT security administrator, forensic analyst, or malware researcher looking to secure against malicious software or investigate malicious code, this book is for you. Prior programming experience and a fair understanding of malware attacks and investigation is expected.

Malware Data Science Joshua Saxe 2018-09-25 Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a "big data" problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you'll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Saxe introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You'll learn how to: - Analyze malware using static analysis - Observe malware behavior using dynamic analysis - Identify adversary groups through shared code analysis - Catch 0-day vulnerabilities by building your own machine learning detector - Measure malware detector accuracy - Identify malware campaigns, trends, and relationships through data visualization Whether you're a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.

The Art of Memory Forensics Michael Hale Ligh 2014-07-22 Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Malware Detection Mihai Christodorescu 2007-03-06 This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Practical Malware Analysis Michael Sikorski 2012-02-01 Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by

professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: –Set up a safe virtual environment to analyze malware –Quickly extract network signatures and host-based indicators –Use key analysis tools like IDA Pro, OllyDbg, and WinDbg –Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques –Use your newfound knowledge of Windows internals for malware analysis –Develop a methodology for unpacking malware and get practical experience with five of the most popular packers –Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

Android Malware and Analysis Ken Dunham 2014-10-24 The rapid growth and development of Android-based devices has resulted in a wealth of sensitive information on mobile devices that offer minimal malware protection. This has created an immediate need for security professionals that understand how to best approach the subject of Android malware threats and analysis.In Android Malware and Analysis, K

A Guide to Forensic Testimony Fred Chris Smith 2003 A technical expert and a lawyer provide practical approaches for IT professionals who need to get up to speed on the role of an expert witness and how testimony works. Includes actual transcripts and case studies.

Practical Memory Forensics Svetlana Ostrovskaya 2022-03-17 A practical guide to enhancing your digital investigations with cutting-edge memory forensics techniques Key FeaturesExplore memory forensics, one of the vital branches of digital investigationLearn the art of user activities reconstruction and malware detection using volatile memoryGet acquainted with a range of open-source tools and techniques for memory forensicsBook Description Memory Forensics is a powerful analysis technique that can be used in different areas, from incident response to malware analysis. With memory forensics, you can not only gain key insights into the user's context but also look for unique traces of malware, in some cases, to piece together the puzzle of a sophisticated targeted attack. Starting with an introduction to memory forensics, this book will gradually take you through more modern concepts of hunting and investigating advanced malware using free tools and memory analysis frameworks. This book takes a practical approach and uses memory images from real incidents to help you gain a better understanding of the subject and develop the skills required to investigate and respond to malware-related incidents and complex targeted attacks. You'll cover Windows, Linux, and macOS internals and explore techniques and tools to detect, investigate, and hunt threats using memory forensics. Equipped with this knowledge, you'll be able to create and analyze memory dumps on your own, examine user activity, detect traces of fileless and memory-based malware, and reconstruct the actions taken by threat actors. By the end of this book, you'll be well-versed in memory forensics and have gained hands-on experience of using various tools associated with it. What you will

learnUnderstand the fundamental concepts of memory organizationDiscover how to perform a forensic investigation of random access memoryCreate full memory dumps as well as dumps of individual processes in Windows, Linux, and macOSAnalyze hibernation files, swap files, and crash dumpsApply various methods to analyze user activitiesUse multiple approaches to search for traces of malicious activityReconstruct threat actor tactics and techniques using random access memory analysisWho this book is for This book is for incident responders, digital forensic specialists, cybersecurity analysts, system administrators, malware analysts, students, and curious security professionals new to this field and interested in learning memory forensics. A basic understanding of malware and its working is expected. Although not mandatory, knowledge of operating systems internals will be helpful. For those new to this field, the book covers all the necessary concepts.

Practical Windows Forensics Ayman Shaaban 2016-06-29 Leverage the power of digital forensics for Windows systems About This Book Build your own lab environment to analyze forensic data and practice techniques. This book offers meticulous coverage with an example-driven approach and helps you build the key skills of performing forensics on Windows-based systems using digital artifacts. It uses specific open source and Linux-based tools so you can become proficient at analyzing forensic data and upgrade your existing knowledge. Who This Book Is For This book targets forensic analysts and professionals who would like to develop skills in digital forensic analysis for the Windows platform. You will acquire proficiency, knowledge, and core skills to undertake forensic analysis of digital data. Prior experience of information security and forensic analysis would be helpful. You will gain knowledge and an understanding of performing forensic analysis with tools especially built for the Windows platform. What You Will Learn Perform live analysis on victim or suspect Windows systems locally or remotely Understand the different natures and acquisition techniques of volatile and non-volatile data. Create a timeline of all the system actions to restore the history of an incident. Recover and analyze data from FAT and NTFS file systems. Make use of various tools to perform registry analysis. Track a system user's browser and e-mail activities to prove or refute some hypotheses. Get to know how to dump and analyze computer memory. In Detail Over the last few years, the wave of the cybercrime has risen rapidly. We have witnessed many major attacks on the governmental, military, financial, and media sectors. Tracking all these attacks and crimes requires a deep understanding of operating system operations, how to extract evident data from digital evidence, and the best usage of the digital forensic tools and techniques. Regardless of your level of experience in the field of information security in general, this book will fully introduce you to digital forensics. It will provide you with the knowledge needed to assemble different types of evidence effectively, and walk you through the various stages of the analysis process. We start by discussing the principles of the digital forensics process and move on to show you the approaches that are used to conduct analysis. We will then study various tools to perform live analysis, and go through different techniques to analyze volatile and non-volatile data. Style and approach This is a step-by-step guide that delivers knowledge about different Windows artifacts. Each topic is explained sequentially, including artifact analysis using different tools and techniques. These techniques make use of the evidence extracted from infected machines, and are accompanied by real-life examples.

Mastering Reverse Engineering Reginald Wong 2018-10-31 Implement reverse engineering techniques to analyze software, exploit software targets, and

defend against security threats like malware and viruses. Key FeaturesAnalyze and improvise software and hardware with real-world examplesLearn advanced debugging and patching techniques with tools such as IDA Pro, x86dbg, and Radare2.Explore modern security techniques to identify, exploit, and avoid cyber threatsBook Description If you want to analyze software in order to exploit its weaknesses and strengthen its defenses, then you should explore reverse engineering. Reverse Engineering is a hackerfriendly tool used to expose security flaws and questionable privacy practices.In this book, you will learn how to analyse software even without having access to its source code or design documents. You will start off by learning the low-level language used to communicate with the computer and then move on to covering reverse engineering techniques. Next, you will explore analysis techniques using real-world tools such as IDA Pro and x86dbg. As you progress through the chapters, you will walk through use cases encountered in reverse engineering, such as encryption and compression, used to obfuscate code, and how to to identify and overcome anti-debugging and anti-analysis tricks. Lastly, you will learn how to analyse other types of files that contain code. By the end of this book, you will have the confidence to perform reverse engineering. What you will learnLearn core reverse engineeringIdentify and extract malware componentsExplore the tools used for reverse engineeringRun programs under non-native operating systemsUnderstand binary obfuscation techniquesIdentify and analyze anti-debugging and anti-analysis tricksWho this book is for If you are a security engineer or analyst or a system programmer and want to use reverse engineering to improve your software and hardware, this is the book for you. You will also find this book useful if you are a developer who wants to explore and learn reverse engineering. Having some programming/shell scripting knowledge is an added advantage.

Python Digital Forensics Cookbook Preston Miller 2017-09-26 Over 60 recipes to help you learn digital forensics and leverage Python scripts to amplify your examinations About This Book Develop code that extracts vital information from everyday forensic acquisitions. Increase the quality and efficiency of your forensic analysis. Leverage the latest resources and capabilities available to the forensic community. Who This Book Is For If you are a digital forensics examiner, cyber security specialist, or analyst at heart, understand the basics of Python, and want to take it to the next level, this is the book for you. Along the way, you will be introduced to a number of libraries suitable for parsing forensic artifacts. Readers will be able to use and build upon the scripts we develop to elevate their analysis. What You Will Learn Understand how Python can enhance digital forensics and investigations Learn to access the contents of, and process, forensic evidence containers Explore malware through automated static analysis Extract and review message contents from a variety of email formats Add depth and context to discovered IP addresses and domains through various Application Program Interfaces (APIs) Delve into mobile forensics and recover deleted messages from SQLite databases Index large logs into a platform to better query and visualize datasets In Detail Technology plays an increasingly large role in our daily lives and shows no sign of stopping. Now, more than ever, it is paramount that an investigator develops programming expertise to deal with increasingly large datasets. By leveraging the Python recipes explored throughout this book, we make the complex simple, quickly extracting relevant information from large datasets. You will explore, develop, and deploy Python code and libraries to provide meaningful results that can be immediately applied to your investigations. Throughout the Python Digital Forensics Cookbook, recipes include topics such as working with forensic evidence containers, parsing mobile and desktop operating system

artifacts, extracting embedded metadata from documents and executables, and identifying indicators of compromise. You will also learn to integrate scripts with Application Program Interfaces (APIs) such as VirusTotal and PassiveTotal, and tools such as Axiom, Cellebrite, and EnCase. By the end of the book, you will have a sound understanding of Python and how you can use it to process artifacts in your investigations. Style and approach Our succinct recipes take a no-frills approach to solving common challenges faced in investigations. The code in this book covers a wide range of artifacts and data sources. These examples will help improve the accuracy and efficiency of your analysis—no matter the situation.

Malware Analysis Techniques Dylan Barker 2021-06-18 Analyze malicious samples, write reports, and use industry-standard methodologies to confidently triage and analyze adversarial software and malware Key FeaturesInvestigate, detect, and respond to various types of malware threatUnderstand how to use what you've learned as an analyst to produce actionable IOCs and reportingExplore complete solutions, detailed walkthroughs, and case studies of real-world malware samplesBook Description Malicious software poses a threat to every enterprise globally. Its growth is costing businesses millions of dollars due to currency theft as a result of ransomware and lost productivity. With this book, you'll learn how to quickly triage, identify, attribute, and remediate threats using proven analysis techniques. Malware Analysis Techniques begins with an overview of the nature of malware, the current threat landscape, and its impact on businesses. Once you've covered the basics of malware, you'll move on to discover more about the technical nature of malicious software, including static characteristics and dynamic attack methods within the MITRE ATT&CK framework. You'll also find out how to perform practical malware analysis by applying all that you've learned to attribute the malware to a specific threat and weaponize the adversary's indicators of compromise (IOCs) and methodology against them to prevent them from attacking. Finally, you'll get to grips with common tooling utilized by professional malware analysts and understand the basics of reverse engineering with the NSA's Ghidra platform. By the end of this malware analysis book, you'll be able to perform in-depth static and dynamic analysis and automate key tasks for improved defense against attacks. What you will learnDiscover how to maintain a safe analysis environment for malware samplesGet to grips with static and dynamic analysis techniques for collecting IOCsReverse-engineer and debug malware to understand its purposeDevelop a well-polished workflow for malware analysisUnderstand when and where to implement automation to react quickly to threatsPerform malware analysis tasks such as code analysis and API inspectionWho this book is for This book is for incident response professionals, malware analysts, and researchers who want to sharpen their skillset or are looking for a reference for common static and dynamic analysis techniques. Beginners will also find this book useful to get started with learning about malware analysis. Basic knowledge of command-line interfaces, familiarity with Windows and Unix-like filesystems and registries, and experience in scripting languages such as PowerShell, Python, or Ruby will assist with understanding the concepts covered.

Mastering Python Forensics Dr. Michael Spreitzenbarth 2015-10-30 Master the art of digital forensics and analysis with Python About This Book Learn to perform forensic analysis and investigations with the help of Python, and gain an advanced understanding of the various Python libraries and frameworks Analyze Python scripts to extract metadata and investigate forensic artifacts The writers, Dr. Michael Spreitzenbarth and Dr. Johann Uhrmann, have used their

experience to craft this hands-on guide to using Python for forensic analysis and investigations Who This Book Is For If you are a network security professional or forensics analyst who wants to gain a deeper understanding of performing forensic analysis with Python, then this book is for you. Some Python experience would be helpful. What You Will Learn Explore the forensic analysis of different platforms such as Windows, Android, and vSphere Semi-automatically reconstruct major parts of the system activity and time-line Leverage Python ctypes for protocol decoding Examine artifacts from mobile, Skype, and browsers Discover how to utilize Python to improve the focus of your analysis Investigate in volatile memory with the help of volatility on the Android and Linux platforms In Detail Digital forensic analysis is the process of examining and extracting data digitally and examining it. Python has the combination of power, expressiveness, and ease of use that makes it an essential complementary tool to the traditional, off-the-shelf digital forensic tools. This book will teach you how to perform forensic analysis and investigations by exploring the capabilities of various Python libraries. The book starts by explaining the building blocks of the Python programming language, especially ctypes in-depth, along with how to automate typical tasks in file system analysis, common correlation tasks to discover anomalies, as well as templates for investigations. Next, we'll show you cryptographic algorithms that can be used during forensic investigations to check for known files or to compare suspicious files with online services such as VirusTotal or Mobile-Sandbox. Moving on, you'll learn how to sniff on the network, generate and analyze network flows, and perform log correlation with the help of Python scripts and tools. You'll get to know about the concepts of virtualization and how virtualization influences IT forensics, and you'll discover how to perform forensic analysis of a jailbroken/rooted mobile device that is based on iOS or Android. Finally, the book teaches you how to analyze volatile memory and search for known malware samples based on YARA rules. Style and approach This easy-to-follow guide will demonstrate forensic analysis techniques by showing you how to solve real-word-scenarios step by step.

Malware Forensics Cameron H. Malin 2008-08-08 Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code. The book gives deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter. This book is

intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code. * Winner of Best Book Bejtlich read in 2008! * http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html * Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader. * First book to detail how to perform "live forensic" techniques on malicous code. * In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Learning Malware Analysis Monnappa K A 2018-06-29 Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Learning Malware Analysis Monnappa K A 2018-06-29 Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting,

responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Malware Analysis and Detection Engineering Abhijit Mohanta 2020-11-05 Discover how the internals of malware work and how you can analyze and detect it. You will learn not only how to analyze and reverse malware, but also how to classify and categorize it, giving you insight into the intent of the malware. Malware Analysis and Detection Engineering is a one-stop guide to malware analysis that simplifies the topic by teaching you undocumented tricks used by analysts in the industry. You will be able to extend your expertise to analyze and reverse the challenges that malicious software throws at you. The book starts with an introduction to malware analysis and reverse engineering to provide insight on the different types of malware and also the terminology used in the anti-malware industry. You will know how to set up an isolated lab environment to safely execute and analyze malware. You will learn about malware packing, code injection, and process hollowing plus how to analyze, reverse, classify, and categorize malware using static and dynamic tools. You will be able to automate your malware analysis process by exploring detection tools to modify and trace malware programs, including sandboxes, IDS/IPS, anti-virus, and Windows binary instrumentation. The book provides comprehensive content in combination with hands-on exercises to help you dig into the details of malware dissection, giving you the confidence to tackle malware that enters your environment. What You Will Learn Analyze, dissect, reverse engineer, and classify malware Effectively handle malware with custom packers and compilers Unpack complex malware to locate vital malware components and decipher their intent Use various static and dynamic malware analysis tools Leverage the internals of various detection engineering tools to improve your workflow Write Snort rules and learn to use them with Suricata IDS Who This Book Is For Security professionals, malware analysts, SOC analysts, incident responders, detection engineers, reverse engineers, and network security engineers "This book is a beast! If you're looking to master the ever-widening field of malware analysis, look no further. This is the definitive guide for you." Pedram Amini, CTO Inquest; Founder OpenRCE.org and ZeroDayInitiative

The Ghidra Book Chris Eagle 2020-09-08 A guide to using the Ghidra software reverse engineering tool suite. The result of more than a decade of research and development within the NSA, the Ghidra platform was developed to address some of the agency's most challenging reverse-engineering problems. With the open-source release of this formerly restricted tool suite, one of the world's most capable disassemblers and intuitive decompilers is now in the hands of cybersecurity defenders everywhere -- and The Ghidra Book is the one and only guide you need to master it. In addition to discussing RE techniques useful in analyzing software and malware of all kinds, the book thoroughly introduces Ghidra's components, features, and unique capacity for group collaboration. You'll learn how to: • Navigate a disassembly • Use Ghidra's built-in decompiler to expedite analysis • Analyze obfuscated binaries • Extend Ghidra to recognize new data types • Build new Ghidra analyzers and loaders • Add support for new processors and instruction sets • Script Ghidra tasks to automate workflows • Set up and use a collaborative reverse engineering environment Designed for beginner and advanced users alike, The Ghidra Book will effectively prepare you to meet the needs and challenges of RE, so you can analyze files like a pro.

Digital Forensics and Incident Response Gerard Johansen 2020-01-29 Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking

fundamentals are required to get started with this book.

Digital Forensics and Incident Response Gerard Johansen 2017-07-24 A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

Hands-On Network Forensics Nipun Jaswal 2019-03-30 Gain basic skills in network forensics and learn how to apply them effectively Key FeaturesInvestigate network threats with easePractice forensics tasks such as intrusion detection, network analysis, and scanningLearn forensics investigation at the network levelBook Description Network forensics is a subset of digital forensics that deals with network attacks and their investigation. In the era of network attacks and malware threat, it’s now more important than ever to have skills to investigate network attacks and vulnerabilities. Hands-On Network Forensics starts with the core concepts within network forensics, including coding, networking, forensics tools, and methodologies for forensic investigations. You’ll then explore the tools used for network forensics, followed by understanding how to apply those tools to a PCAP file and write the accompanying report. In addition to this, you will understand how statistical flow analysis, network enumeration, tunneling and encryption, and malware detection can be used to investigate your network. Towards the end of this book, you will discover how network correlation works and how to bring all the information from different types of network devices together. By the end of

this book, you will have gained hands-on experience of performing forensics analysis tasks. What you will learnDiscover and interpret encrypted trafficLearn about various protocolsUnderstand the malware language over wireGain insights into the most widely used malwareCorrelate data collected from attacksDevelop tools and custom scripts for network forensics automationWho this book is for The book targets incident responders, network engineers, analysts, forensic engineers and network administrators who want to extend their knowledge from the surface to the deep levels of understanding the science behind network protocols, critical indicators in an incident and conducting a forensic search over the wire.

Rootkits Greg Hoglund 2006 A guide to rootkits describes what they are, how they work, how to build them, and how to detect them.

Malware Ed Skoudis 2004 Describes various types of malware, including viruses, worms, user-level RootKits, and kernel-level manipulation, their haracteristics and attack method, and how to defend against an attack.