

Malware Analysis Sandbox

Mobile Malware Attacks and Defense *Cuckoo Malware Analysis Information Science and Applications (ICISA) 2016 Operationalizing Threat Intelligence Android Malware and Analysis Recent Advances in Intrusion Detection Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit Research in Attacks, Intrusions, and Defenses Information and Communications Security Malware Forensics Field Guide for Linux Systems Handbook of Research on Machine and Deep Learning Applications for Cyber Security Detection of Intrusions and Malware, and Vulnerability Assessment Computer Security - ESORICS 2017 International Conference on Security and Privacy in Communication Networks Windows Malware Analysis Essentials Recent Advances in Computational Intelligence in Defense and Security Malware Forensics Field Guide for Windows Systems Research Anthology on Securing Mobile Technologies and Applications The Network Security Test Lab Information Systems Security Advances in Biometrics Learning Android Forensics Computing Science, Communication and Security E-Business and Telecommunications Security and Privacy in Communication Networks Botnets Applied Incident Response Research in Attacks, Intrusions, and Defenses Digital Forensics and Cyber Crime Cyber-Security Threats, Actors, and Dynamic Mitigation Virtual Honeyspots Proceedings of the International Conference on Paradigms of Communication, Computing and Data Sciences Cisco Certified CyberOps Associate 200-201 Certification Guide Cyber Security and Computer Science Pervasive Computing and the Networked World Digital Forensics and Incident Response Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications Knowledge Engineering and Management Information Security Theory and Practice Proceedings of International Conference on Artificial Intelligence and Applications*

Recognizing the pretentiousness ways to acquire this books Malware Analysis Sandbox is additionally useful. You have remained in right site to begin getting this info. get the Malware Analysis Sandbox join that we find the money for here and check out the link.

You could purchase guide Malware Analysis Sandbox or acquire it as soon as feasible. You could quickly download this Malware Analysis Sandbox after getting deal. So, later you require the books swiftly, you can straight get it. Its correspondingly completely simple and correspondingly fats, isnt it? You have to favor to in this reveal

Digital Forensics and Cyber Crime Jun 07 2020 This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2012, held in October 2012 in Lafayette, Indiana, USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybercrime investigations.

Knowledge Engineering and Management Aug 29 2019 These proceedings present technical papers selected from the 2012 International Conference on Intelligent Systems and Knowledge Engineering (ISKE 2012), held on December 15-17 in Beijing. The aim of this conference is to bring together experts from different fields of expertise to discuss the state-of-the-art in Intelligent Systems and Knowledge Engineering, and to present new findings and perspectives on future developments. The proceedings introduce current scientific and technical advances in the fields of artificial intelligence, machine learning, pattern recognition, data mining, knowledge engineering, information retrieval, information theory, knowledge-based systems, knowledge representation and reasoning, multi-agent systems, and natural-language processing, etc. Furthermore they include papers on new intelligent computing paradigms, which combine new computing methodologies, e.g., cloud computing, service computing and pervasive computing with traditional intelligent methods. By presenting new methodologies and practices, the proceedings will benefit both researchers and practitioners who want to utilize intelligent methods in their specific fields. Dr. Fuchun Sun is a professor at the Department of Computer Science & Technology, Tsinghua University, China. Dr. Tianrui Li is a professor at the School of Information Science & Technology, Southwest Jiaotong University, Chengdu, China. Dr. Hongbo Li also works at the Department of Computer Science & Technology, Tsinghua University, China.

Information and Communications Security Feb 25 2022 This book constitutes the refereed proceedings of the 21th International Conference on Information and Communications Security, ICICS 2019, held in Beijing, China, in December 2019. The 47 revised full papers were carefully selected from 199 submissions. The papers are organized in topics on malware analysis and detection, IoT and CPS security enterprise network security, software security, system security, authentication, applied cryptograph internet security, machine learning security, machine learning privacy, Web security, steganography and steganalysis.

Virtual Honeyspots Apr 05 2020 Honeyspots have demonstrated immense value in Internet security, but physical honeypot deployment can be prohibitively complex, time-consuming, and expensive. Now, there's a breakthrough solution. Virtual honeypots share many attributes of traditional honeypots, but you can run thousands of them on a single system-making them easier and cheaper to build, deploy, and maintain. In this hands-on, highly accessible book, two leading honeypot pioneers systematically introduce virtual honeypot technology. One step at a time, you'll learn exactly how to implement, configure, use, and maintain virtual honeypots in your own environment, even if you've never deployed a honeypot before. You'll learn through examples, including Honeyd, the acclaimed virtual honeypot created by coauthor Niels Provos. The authors also present multiple real-world applications for virtual honeypots, including network decoy, worm detection, spam prevention, and network simulation. After reading this book, you will be able to Compare high-interaction honeypots that provide real systems and services and the low-interaction honeypots that emulate them Install and configure Honeyd to simulate multiple operating systems, services, and network environments Use virtual honeypots to capture worms, bots, and other malware Create high-performance "hybrid" honeypots that draw on technologies from both low- and high-interaction honeypots Implement client honeypots that actively seek out dangerous Internet locations Understand how attackers identify and circumvent honeypots Analyze the botnets your honeypot identifies, and the malware it captures Preview the future evolution of both virtual and physical honeypots

Learning Android Forensics Jan 15 2021 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.

Computer Security - ESORICS 2017 Oct 24 2021 The two-volume set, LNCS 10492 and LNCS 10493 constitutes the refereed proceedings of the 22nd European Symposium on Research in Computer Security, ESORICS 2017, held in Oslo, Norway, in September 2017. The 54 revised full papers presented were carefully reviewed and selected from 338 submissions. The papers address issues such as data protection; security protocols; systems; web and network security; privacy; threat modeling and detection; information flow; and security in emerging applications such as cryptocurrencies, the Internet of Things and automotive.

Windows Malware Analysis Essentials Aug 22 2021 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 code in 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.

Cisco Certified CyberOps Associate 200-201 Certification Guide Feb 02 2020 Begin a successful career in cybersecurity operations by achieving Cisco Certified CyberOps Associate 200-201 certification Key Features Receive expert guidance on how to kickstart your career in the cybersecurity industry Gain hands-on experience while studying for the Cisco Certified CyberOps Associate certification exam Work through practical labs and exercises mapped directly to the exam objectives Book Description Achieving the Cisco Certified CyberOps Associate 200-201 certification helps you to kickstart your career in cybersecurity operations. This book offers up-to-date coverage of 200-201 exam resources to fully equip you to pass on your first attempt. The book covers the essentials of network security concepts and shows you how to perform security threat monitoring. You'll begin by gaining an in-depth understanding of cryptography and exploring the methodology for performing both host and network-based intrusion analysis. Next, you'll learn about the importance of implementing security management and incident response strategies in an enterprise organization. As you advance, you'll see why implementing defenses is necessary by taking an in-depth approach, and then perform security monitoring and packet analysis on a network. You'll also discover the need for computer forensics and get to grips with the components used to identify network intrusions. Finally, the book will not only help you to learn the theory but also enable you to gain much-needed practical experience for the cybersecurity industry. By the end of this Cisco cybersecurity book, you'll have covered everything you need to pass the Cisco Certified CyberOps Associate 200-201 certification exam, and have a handy, on-the-job desktop reference guide. What you will learn Incorporate security into your architecture to prevent attacks Discover how to implement and prepare secure designs Identify access control models for digital assets Identify point of entry, determine scope, contain threats, and remediate Find out how to perform malware analysis and interpretation Implement security technologies to detect and analyze threats Who this book is for This book is for students who want to pursue a career in cybersecurity operations, threat detection and analysis, and incident response. IT professionals, network security engineers, security operations center (SOC) engineers, and cybersecurity analysts looking for a career boost and those looking to get certified in Cisco cybersecurity technologies and break into the cybersecurity industry will also benefit from this book. No prior knowledge of IT networking and cybersecurity industries is needed.

Android Malware and Analysis Jul 01 2022 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, Ken Dunham, renowned global malware expert and author, teams up with international experts to document the best tools and tactics available for analyzing Android malware. The book covers both methods of malware analysis: dynamic and static. This tactical and practical book shows you how to use to use dynamic malware analysis to check the behavior of an application/malware as it has been executed in the system. It also describes how you can apply static analysis to break apart the application/malware using reverse engineering tools and techniques to recreate the actual code and algorithms used. The book presents the insights of experts in the field, who have already sized up the best tools, tactics, and procedures for recognizing and analyzing Android malware threats quickly and effectively. You also get access to an online library of tools that supplies what you will need to begin your own analysis of Android malware threats. Tools available on the book's site include updated information, tutorials, code, scripts, and author assistance. This is not a book on Android OS, fuzz testing, or social engineering. Instead, it is about the best ways to analyze and tear apart Android malware threats. After reading the book, you will be able to immediately implement the tools and tactics covered to identify and analyze the latest evolution of Android threats. Updated information, tutorials, a private forum, code, scripts, tools, and author assistance are available at AndroidRisk.com for first-time owners of the book.

Pervasive Computing and the Networked World Dec 02 2019 This book constitutes the refereed post-proceedings of the Joint International Conference on Pervasive Computing and the Networked World, ICPCN-SWS 2012, held in Istanbul, Turkey, in November 2012. This conference is a merger of the 7th International Conference on Pervasive Computing and Applications (ICPCA) and the 4th Symposium on Web Society (SWS). The 53 revised full papers and 26 short papers presented were carefully reviewed and selected from 143 submissions. The papers cover a wide range of topics from different research communities such as computer science, sociology and psychology and explore both theoretical and practical issues in and around the emerging computing paradigms, e.g., pervasive collaboration, collaborative business, and networked societies. They highlight the unique characteristics of the "everywhere" computing paradigm and promote the awareness of its potential social and psychological consequences.

Computing Science, Communication and Security Dec 14 2020 This book constitutes revised selected papers of the Third International Conference on Computing Science, Communication and Security, COMS2 2022, held in Gandhinagar, India, in February 2022. Due to the COVID-19 pandemic the conference was held virtually. The 22 full papers were thoroughly reviewed and selected from 143 submissions. The papers present ideas, and research results on the aspects of computing science, network communication, and security.

Cyber-Security Threats, Actors, and Dynamic Mitigation May 07 2020 Cyber-Security Threats, Actors, and Dynamic Mitigation provides both a technical and state-of-the-art perspective as well as a systematic overview of the recent advances in different facets of cyber-security. It covers the methodologies for modeling attack strategies used by threat actors targeting devices, systems, and networks such as smart homes, critical infrastructures, and industrial IoT. With a comprehensive review of the threat landscape, the book explores both common and sophisticated threats to systems and networks. Tools and methodologies are presented for precise modeling of attack strategies, which can be used both proactively in risk management and reactively in intrusion prevention and response systems. Several contemporary techniques are offered ranging from reconnaissance and penetration testing to malware detection, analysis, and mitigation. Advanced machine learning-based approaches are also included in the area of anomaly-based detection, that are capable of detecting attacks relying on zero-day vulnerabilities and exploits. Academics, researchers, and professionals in cyber-security who want an in-depth look at the contemporary aspects of the field will find this book of interest. Those wanting a unique reference for various cyber-security threats and how they are detected, analyzed, and mitigated will reach for this book often.

Cyber Security and Computer Science Jan 03 2020 This book constitutes the refereed post-conference proceedings of the Second International Conference on Cyber Security and Computer Science, ICONCS 2020, held in Dhaka, Bangladesh, in February 2020. The 58 full papers were carefully reviewed and selected from 133 submissions. The papers detail new ideas, inventions, and application experiences to cyber security systems. They are organized in topical sections on optimization problems; image steganography and risk analysis on web applications; machine learning in disease diagnosis and monitoring; computer vision and image processing in health care; text and speech processing; machine learning in health care; blockchain applications; computer vision and image processing in health care; malware analysis; computer vision; future technology applications; computer networks; machine learning on imbalanced data; computer security; Bangla language processing.

Malware Forensics Field Guide for Windows Systems Jun 19 2021 Malware Forensics Field Guide for Windows Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Windows-based systems, the largest running OS in the world. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program. This field guide is intended for computer forensic investigators, analysts, and specialists. 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

Proceedings of International Conference on Artificial Intelligence and Applications Jun 27 2019 This book gathers high-quality papers presented at the International Conference on Artificial Intelligence and Applications (ICAIA 2020), held at Maharaja Surajmal Institute of Technology, New Delhi, India, on 6-7 February 2020. The book covers areas such as artificial neural networks, fuzzy systems, computational optimization technologies and machine learning.

Advances in Biometrics Feb 13 2021 This book provides a framework for robust and novel biometric techniques, along with implementation and design strategies. The theory, principles, pragmatic and modern methods, and future directions of biometrics are presented, along with in-depth coverage of biometric applications in driverless cars, automated and AI-based systems, IoT, and wearable devices. Additional coverage includes computer vision and pattern recognition, cybersecurity, cognitive computing, soft biometrics, and the social impact of biometric technology. The book will be a valuable reference for researchers, faculty, and practicing professionals working in biometrics and related fields, such as image processing, computer vision, and artificial intelligence. Highlights robust and novel biometric techniques Provides implementation strategies and future research directions in the field of biometrics Includes case studies and emerging applications

Handbook of Research on Machine and Deep Learning Applications for Cyber Security Dec 26 2021 As the advancement of technology continues, cyber security continues to play a significant role in today's world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications Sep 30 2019 The book is a collection of high-quality peer-reviewed research papers presented at International Conference on Frontiers of Intelligent Computing: Theory and applications (FICTA 2016) held at School of Computer Engineering, KIIT University, Bhubaneswar, India during 16 - 17 September 2016. The book presents theories, methodologies, new ideas, experiences and applications in all areas of intelligent computing and its applications to various engineering disciplines like computer science, electronics, electrical and mechanical engineering.

E-Business and Telecommunications Nov 12 2020 This book constitutes the refereed proceedings of the 13th International Joint Conference on E-Business and Telecommunications, ICETE 2016, held in Lisbon, Portugal, in July 2016. ICETE is a joint international conference integrating four major areas of knowledge that are divided into six corresponding conferences: International Conference on Data Communication Networking, DCNET; International Conference on E-Business, ICE-B; International Conference on Optical Communication Systems, OPTICS; International Conference on Security and Cryptography, SECRYPT; International Conference on Signal Processing and Multimedia, SIGMAP; International Conference on Wireless Information Systems, WINSYS. The 20 full papers presented together with an invited paper in this volume were carefully reviewed and selected from 241 submissions. The papers cover the following key areas of e-business and telecommunications: data communication networking; e-business; optical communication systems; security and cryptography; signal processing and multimedia applications; wireless networks and mobile systems.

Digital Forensics and Incident Response Oct 31 2019 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.

Recent Advances in Intrusion Detection May 31 2022 This book constitutes the proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection, RAID 2011, held in Menlo Park, CA, USA in September 2011. The 20 papers presented were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on application security; malware; anomaly detection; Web security and social networks; and sandboxing and embedded environments.

Research in Attacks, Intrusions, and Defenses Jul 09 2020 This book constitutes the refereed conference proceedings of the 20th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2017, held in Atlanta, GA, USA, in September 2017. The 21 revised full papers were selected from 105 submissions. They are organized in the following topics: software security, intrusion detection, systems security, android security, cybercrime, cloud security, network security.

Mobile Malware Attacks and Defense Nov 05 2022 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 threats. * 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

Proceedings of the International Conference on Paradigms of Communication, Computing and Data Sciences Mar 05 2020 This book gathers selected high-quality research papers presented at the International Conference on Paradigms of Communication, Computing and Data Sciences (PCCDS 2021), held at the National Institute of Technology, Kurukshetra, India, during May 07-09, 2021. It discusses high-quality and cutting-edge research in the areas of advanced computing, communications, and data science techniques. The book is a collection of latest research articles in computation algorithm, communication, and data sciences, intertwined with each other for efficiency.

Cuckoo Malware Analysis Oct 04 2022 This book is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This book features clear and concise guidance in an easily accessible format. Cuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analysing malware effectively and efficiently.

Security and Privacy in Communication Networks Oct 12 2020 This two-volume set LNCS 398 and 399 constitutes the post-conference proceedings of the 17th International Conference on Security and Privacy in Communication Networks, SecureComm 2021, held in September 2021. Due to COVID-19 pandemic the conference was held virtually. The 56 full papers were carefully reviewed and selected from 143 submissions. The papers focus on the latest scientific research results in security and privacy in wired, mobile, hybrid and ad hoc networks, in IoT technologies, in cyber-physical systems, in next-generation communication systems in web and systems security and in pervasive and ubiquitous computing.

Research Anthology on Securing Mobile Technologies and Applications May 19 2021 Mobile technologies have become a staple in society for their accessibility and diverse range of applications that are continually growing and advancing. Users are increasingly using these devices for activities beyond simple communication including gaming and e-commerce and to access confidential information including banking accounts and medical records. While mobile devices are being so widely used and accepted in daily life, and subsequently housing more and more personal data, it is evident that the security of these devices is paramount. As mobile applications now create easy access to personal information, they can incorporate location tracking services, and data collection can happen discreetly behind the scenes. Hence, there needs to be more security and privacy measures enacted to ensure that mobile technologies can be used safely. Advancements in trust and privacy, defensive strategies, and steps for securing the device are important foci as mobile technologies are highly popular and rapidly developing. The Research Anthology on Securing

Mobile Technologies and Applications discusses the strategies, methods, and technologies being employed for security amongst mobile devices and applications. This comprehensive book explores the security support that needs to be required on mobile devices to avoid application damage, hacking, security breaches and attacks, or unauthorized accesses to personal data. The chapters cover the latest technologies that are being used such as cryptography, verification systems, security policies and contracts, and general network security procedures along with a look into cybercrime and forensics. This book is essential for software engineers, app developers, computer scientists, security and IT professionals, practitioners, stakeholders, researchers, academicians, and students interested in how mobile technologies and applications are implementing security protocols and tactics amongst devices.

Botnets Sep 10 2020 The book begins with real world cases of botnet attacks to underscore the need for action. Next the book will explain botnet fundamentals using real world examples. These chapters will cover what they are, how they operate, and the environment and technology that makes them possible. The following chapters will analyze botnets for opportunities to detect, track, and remove them. Then the book will describe intelligence gathering efforts and results obtained to date. Public domain tools like OurMon, developed by Jim Binkley of Portland State University, will be described in detail along with discussions of other tools and resources that are useful in the fight against Botnets. This is the first book to explain the newest internet threat - Botnets, zombie armies, bot herders, what is being done, and what you can do to protect your enterprise Botnets are the most complicated and difficult threat the hacker world has unleashed - read how to protect yourself

Recent Advances in Computational Intelligence in Defense and Security Jul 21 2021 This volume is an initiative undertaken by the IEEE Computational Intelligence Society's Task Force on Security, Surveillance and Defense to consolidate and disseminate the role of CI techniques in the design, development and deployment of security and defense solutions. Applications range from the detection of buried explosive hazards in a battlefield to the control of unmanned underwater vehicles, the delivery of superior video analytics for protecting critical infrastructures or the development of stronger intrusion detection systems and the design of military surveillance networks. Defense scientists, industry experts, academicians and practitioners alike will all benefit from the wide spectrum of successful applications compiled in this volume. Senior undergraduate or graduate students may also discover uncharted territory for their own research endeavors.

Information Systems Security Mar 17 2021 This book constitutes the proceedings of the 17th International Conference on Information Systems Security, ICISS 2021, held in Patna, India, during December 16-20, 2021. The 9 regular papers, 2 short papers and 4 work-in-progress papers included in this volume were carefully reviewed and selected from a total of 48 submissions. The papers were organized in topical sections named: attack detection, malware identification, data security in distributed systems, and applied cryptography.

Research in Attacks, Intrusions, and Defenses Mar 29 2022 This book constitutes the refereed proceedings of the 19th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2016, held in Evry, France, in September 2016. The 21 full papers presented were carefully reviewed and selected from 85 submissions. They are organized around the following topics: systems security; low-level attacks and defenses; measurement studies; malware analysis; network security; systematization of knowledge and experience reports; Web and mobile security.

Operationalizing Threat Intelligence Aug 02 2022 Learn cyber threat intelligence fundamentals to implement and operationalize an organizational intelligence program Key Features Develop and implement a threat intelligence program from scratch Discover techniques to perform cyber threat intelligence, collection, and analysis using open-source tools Leverage a combination of theory and practice that will help you prepare a solid foundation for operationalizing threat intelligence programs Book Description We're living in an era where cyber threat intelligence is becoming more important. Cyber threat intelligence routinely informs tactical and strategic decision-making throughout organizational operations. However, finding the right resources on the fundamentals of operationalizing a threat intelligence function can be challenging, and that's where this book helps. In *Operationalizing Threat Intelligence*, you'll explore cyber threat intelligence in five fundamental areas: defining threat intelligence, developing threat intelligence, collecting threat intelligence, enrichment and analysis, and finally production of threat intelligence. You'll start by finding out what threat intelligence is and where it can be applied. Next, you'll discover techniques for performing cyber threat intelligence collection and analysis using open source tools. The book also examines commonly used frameworks and policies as well as fundamental operational security concepts. Later, you'll focus on enriching and analyzing threat intelligence through pivoting and threat hunting. Finally, you'll examine detailed mechanisms for the production of intelligence. By the end of this book, you'll be equipped with the right tools and understand what it takes to operationalize your own threat intelligence function, from collection to production. What you will learn Discover types of threat actors and their common tactics and techniques Understand the core tenets of cyber threat intelligence Discover cyber threat intelligence policies, procedures, and frameworks Explore the fundamentals relating to collecting cyber threat intelligence Understand fundamentals about threat intelligence enrichment and analysis Understand what threat hunting and pivoting are, along with examples Focus on putting threat intelligence into production Explore techniques for performing threat analysis, pivoting, and hunting Who this book is for This book is for cybersecurity professionals, security analysts, security enthusiasts, and anyone who is just getting started and looking to explore threat intelligence in more detail. Those working in different security roles will also be able to explore threat intelligence with the help of this security book.

Applied Incident Response Aug 10 2020 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

Information Security Theory and Practice Jul 29 2019 This volume constitutes the refereed proceedings of the 11th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2017, held in Heraklion, Crete, Greece, in September 2017. The 8 revised full papers and 4 short papers presented were carefully reviewed and selected from 35 submissions. The papers are organized in the following topical sections: security in emerging systems; security of data; trusted execution; defenses and evaluation; and protocols and algorithms.

Malware Forensics Field Guide for Linux Systems Jan 27 2022 Malware Forensics Field Guide for Linux Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program. This book will appeal to computer forensic investigators, analysts, and specialists. A compendium of on-the-job tasks and checklists Specific for Linux-based systems in which new malware is developed every day Authors are world-renowned leaders in investigating and analyzing malicious code

Information Science and Applications (ICISA) 2016 Sep 03 2022 This book contains selected papers from the 7th International Conference on Information Science and Applications (ICISA 2016) and provides a snapshot of the latest issues encountered in technical convergence and convergences of security technology. It explores how information science is core to most current research, industrial and commercial activities and consists of contributions covering topics including Ubiquitous Computing, Networks and Information Systems, Multimedia and Visualization, Middleware and Operating Systems, Security and Privacy, Data Mining and Artificial Intelligence, Software Engineering, and Web Technology. The contributions describe the most recent developments in information technology and ideas, applications and problems related to technology convergence, illustrated through case studies, and reviews converging existing security techniques. Through this volume, readers will gain an understanding of the current state-of-the-art information strategies and technologies of convergence security. The intended readers are researchers in academia, industry and other research institutes focusing on information science and technology.

The Network Security Test Lab Apr 17 2021 The ultimate hands-on guide to IT security and proactive defense The Network Security Test Lab is a hands-on, step-by-step guide to ultimate IT security implementation. Covering the full complement of malware, viruses, and other attack technologies, this essential guide walks you through the security assessment and penetration testing process, and provides the set-up guidance you need to build your own security-testing lab. You'll look inside the actual attacks to decode their methods, and learn how to run attacks in an isolated sandbox to better understand how attacker target systems, and how to build the defenses that stop them. You'll be introduced to tools like Wireshark, NetworkMiner, Nmap, Metasploit, and more as you discover techniques for defending against network attacks, social networking bugs, malware, and the most prevalent malicious traffic. You also get access to open source tools, demo software, and a bootable version of Linux to facilitate hands-on learning and help you implement your new skills. Security technology continues to evolve, and yet not a week goes by without

news of a new security breach or a new exploit being released. The Network Security Test Lab is the ultimate guide when you are on the front lines of defense, providing the most up-to-date methods of thwarting would-be attackers. Get acquainted with your hardware, gear, and test platform. Learn how attackers penetrate existing security systems. Detect malicious activity and build effective defenses. Investigate and analyze attacks to inform defense strategy. The Network Security Test Lab is your complete, essential guide.

International Conference on Security and Privacy in Communication Networks Sep 22 2021 This 2-volume set constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Security and Privacy in Communication Networks, SecureComm 2014, held in Beijing, China, in September 2014. The 27 regular and 17 short papers presented were carefully reviewed. It also presents 22 papers accepted for four workshops (ATCS, SSS, SLSS, DAPRO) in conjunction with the conference, 6 doctoral symposium papers and 8 poster papers. The papers are grouped in the following topics: security and privacy in wired, wireless, mobile, hybrid, sensor, ad hoc networks; network intrusion detection and prevention, firewalls, packet filters; malware, and distributed denial of service; communication privacy and anonymity; network and internet forensics techniques; public key infrastructures, key management, credential management; secure routing, naming/addressing, network management; security and privacy in pervasive and ubiquitous computing; security & privacy for emerging technologies: VoIP, peer-to-peer and overlay network systems; security & isolation in data center networks; security & isolation in software defined networking.

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit Apr 29 2022 This book provides digital forensic investigators, security professionals, and law enforcement with all of the information, tools, and utilities required to conduct forensic investigations of computers running any variant of the Macintosh OS X operating system, as well as the almost ubiquitous iPod and iPhone. Digital forensic investigators and security professionals subsequently can use data gathered from these devices to aid in the prosecution of criminal cases, litigate civil cases, audit adherence to federal regulatory compliance issues, and identify breach of corporate and government usage policies on networks. MAC Disks, Partitioning, and HFS+ File System Manage multiple partitions on a disk, and understand how the operating system stores data. FileVault and Time Machine Decrypt locked FileVault files and restore files backed up with Leopard's Time Machine. Recovering Browser History Uncover traces of Web-surfing activity in Safari with Web cache and .plist files Recovering Email Artifacts, iChat, and Other Chat Logs Expose communications data in iChat, Address Book, Apple's Mail, MobileMe, and Web-based email. Locating and Recovering Photos Use iPhoto, Spotlight, and shadow files to find artifacts of photos (e.g., thumbnails) when the originals no longer exist. Finding and Recovering QuickTime Movies and Other Video Understand video file formats--created with iSight, iMovie, or another application--and how to find them. PDF, Word, and Other Document Recovery Recover text documents and metadata with Microsoft Office, OpenOffice, Entourage, Adobe PDF, or other formats. Forensic Acquisition and Analysis of an iPod Document seizure of an iPod model and analyze the iPod image file and artifacts on a Mac. Forensic Acquisition and Analysis of an iPhone Acquire a physical image of an iPhone or iPod Touch and safely analyze without jailbreaking. Includes Unique Information about Mac OS X, iPod, iMac, and iPhone Forensic Analysis Unavailable Anywhere Else Authors Are Pioneering Researchers in the Field of Macintosh Forensics, with Combined Experience in Law Enforcement, Military, and Corporate Forensics

Detection of Intrusions and Malware, and Vulnerability Assessment Nov 24 2021 This book constitutes the refereed proceedings of the 15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2018, held in Saclay, France, in June 2018. The 17 revised full papers and 1 short paper included in this book were carefully reviewed and selected from 59 submissions. They present topics such as malware analysis; mobile and embedded security; attacks; detection and containment; web and browser security; and reverse engineering.