Linux Malware Incident Response A Practitioners Guide To Forensic Collection And Examination Of Volatile Data An Excerpt From Malware Forensic Field Guide For Linux Systems Author Cameron H Malin Mar 2013

Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support. Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each phase of incident response are explored in the book. Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You'll Learn Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response

plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team Who This Book Is For Cybersecurity leaders, executives, consultants, and entry-level professionals responsible for executing the incident response plan when something goes wrong

This book is a comprehensive guide for organizations on how to prepare for cyber-attacks, control cyber threats and network security breaches in a way that decreases damage, recovery time, and costs, and adapt existing strategies to cloud-based environments.

Become an effective cyber forensics investigator and gain a collection of practical, efficient techniques to get the job done. Diving straight into a discussion of anti-forensic techniques, this book shows you the many ways to effectively detect them. Now that you know what you are looking for, you'll shift your focus to network forensics, where you cover the various tools available to make your network forensics process less complicated. Following this, you will work with cloud and mobile forensic techniques by considering the concept of forensics as a service (FaSS), giving you cutting-edge skills that will future-proof your career. Building on this, you will learn the process of breaking down malware attacks, web attacks, and email scams with case studies to give you a clearer view of the techniques to be followed. Another tricky technique is SSD forensics, so the author covers this in detail to give you the alternative analysis techniques you'll need. To keep you up to speed on contemporary forensics, Practical Cyber

Forensics includes a chapter on Bitcoin forensics, where key crypto-currency forensic techniques will be shared. Finally, you will see how to prepare accurate investigative reports. What You Will Learn Carry out forensic investigation on Windows, Linux, and macOS systems Detect and counter anti-forensic techniques Deploy network, cloud, and mobile forensics Investigate web and malware attacks Write efficient investigative reports Who This Book Is For Intermediate infosec professionals looking for a practical approach to investigative cyber forensics techniques.

An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is a must for all organizations. This book offers concrete and detailed guidance on how to conduct the full spectrum of incident response and digital forensic activities.

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.

Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communication guides readers through the fascinating history and principles of deception—and how these techniques and stratagems are now being effectively used by cyber attackers. Users will find an in-depth guide that provides valuable insights into the cognitive, sensory and narrative bases of misdirection, used to shape the targeted audience's perceptions and beliefs. The text provides a detailed analysis of the psychological, sensory, sociological, and technical precepts that reveal predictors of attacks—and conversely postmortem insight about attackers—presenting a unique resource that empowers readers to observe, understand and protect against cyber deception tactics. Written by information security experts with real-world investigative experience, the text is the most instructional book available on the subject, providing practical guidance to readers with rich literature references, diagrams and examples that enhance the learning process. Deeply examines the psychology of deception through the lens of misdirection and other techniques used by master magicians Explores cognitive vulnerabilities that cyber attackers use to exploit human targets Dissects the underpinnings and elements of deception narratives Examines group dynamics and deception factors in cyber attacker underground markets Provides deep coverage on how cyber attackers leverage psychological influence techniques in the trajectory of deception strategies

Explores the deception strategies used in today's threat landscape—phishing, watering hole, scareware and ransomware attacks Gives unprecedented insight into deceptive Internet video communications Delves into the history and deception pathways of nation-state and cyber terrorism attackers Provides unique insight into honeypot technologies and strategies Explores the future of cyber deception

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 Malware analysis is a powerful investigation technique widely used in various security areas including digital forensics and incident response processes. Working through practical examples, you'll be able to analyze any type of malware you may encounter within the modern world.

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and

those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems

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

when they get in, you'll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be. This Practitioner's Guide is designed to help digital investigators identify malware on a Linux computer system, collect volatile (and relevant nonvolatile) system data to further investigation, and determine the impact malware makes on a subject system, all in a reliable, repeatable, defensible, and thoroughly documented manner.

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 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. The Definitive Guide to File System Analysis: Key

Concepts and Hands-on Techniques Most digital evidence is stored within the computer's file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today's most valuable open source file system analysis tools—including tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk's Host Protected Area (HPA) Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more Analyzing DOS, Apple, and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more

Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools When it comes to file system analysis, no other book offers this much detail or expertise. Whether you're a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use. 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.

Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

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

Every computer crime leaves tracks–you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity.

Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Computer Forensics provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process–from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

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

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset. Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations. Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system,

there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones. Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately. For online source codes, please visit: https://github.com/jbradley89/osx_inc ident_response_scripting_and_analysis Focuses exclusively on OS X attacks, incident response, and forensics Provides the technical details of OS X so you can find artifacts that might be missed using automated tools Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

?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.

Covering up-to-date mobile platforms, this book focuses on teaching you the most recent tools and techniques for investigating mobile devices. Readers will delve into a variety of mobile forensics techniques for iOS 11-13, Android 8-10 devices, and Windows 10.

Gain basic skills in network forensics and learn how to apply them effectively Key Features Investigate network threats with ease Practice forensics tasks such as intrusion detection, network analysis, and scanning Learn forensics investigation at the network level Book 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 learn Discover and interpret encrypted traffic Learn about various protocols Understand the malware language over wire Gain insights into the most widely used malware Correlate data collected from attacks Develop tools and custom scripts for network forensics automation Who 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. Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis,

and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

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 malicioussoftware; 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.

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: –Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies –Protect attached evidence media from accidental modification –Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal –Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping –Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt –Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted

drives using BitLocker, FileVault, and TrueCrypt; and others –Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

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

Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident

response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Packed with real-world examples using freely available open source tools Deep explanation and understanding of the Windows Registry – the most difficult part of Windows to analyze forensically Includes a CD containing code and author-created tools discussed in the book

Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the crucial importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management Identify the key steps to completing a successful

computer incident response investigation Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

A resource to help forensic investigators locate,

analyze, and understand digital evidence found on modern Linux systems after a crime, security incident or cyber attack. Practical Linux Forensics dives into the technical details of analyzing postmortem forensic images of Linux systems which have been misused, abused, or the target of malicious attacks. It helps forensic investigators locate and analyze digital evidence found on Linux desktops, servers, and IoT devices. Throughout the book, you learn how to identify digital artifacts which may be of interest to an investigation, draw logical conclusions, and reconstruct past activity from incidents. You'll learn how Linux works from a digital forensics and investigation perspective, and how to interpret evidence from Linux environments. The techniques shown are intended to be independent of the forensic analysis platforms and tools used. Learn how to: • Extract evidence from storage devices and analyze partition tables, volume managers, popular Linux filesystems (Ext4, Btrfs, and Xfs), and encryption • Investigate evidence from Linux logs, including traditional syslog, the systemd journal, kernel and audit logs, and logs from daemons and applications • Reconstruct the Linux startup process, from boot loaders (UEFI and Grub) and kernel initialization, to systemd unit files and targets leading up to a graphical login • Perform analysis of power, temperature, and the physical environment of a Linux machine, and find evidence of sleep,

hibernation, shutdowns, reboots, and crashes • Examine installed software, including distro installers, package formats, and package management systems from Debian, Fedora, SUSE, Arch, and other distros • Perform analysis of time and Locale settings, internationalization including language and keyboard settings, and geolocation on a Linux system • Reconstruct user login sessions (shell, X11 and Wayland), desktops (Gnome, KDE, and others) and analyze keyrings, wallets, trash cans, clipboards, thumbnails, recent files and other desktop artifacts • Analyze network configuration, including interfaces, addresses, network managers, DNS, wireless artifacts (Wi-Fi, Bluetooth, WWAN), VPNs (including WireGuard), firewalls, and proxy settings • Identify traces of attached peripheral devices (PCI, USB, Thunderbolt, Bluetooth) including external storage, cameras, and mobiles, and reconstruct printing and scanning activity 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.

Develop more secure and effective antivirus solutions by leveraging antivirus bypass techniques Key Features: Gain a clear understanding of the security landscape and research

approaches to bypass antivirus software Become well-versed with practical techniques to bypass antivirus solutions Discover best practices to develop robust antivirus solutions Book Description: Antivirus software is built to detect, prevent, and remove malware from systems, but this does not guarantee the security of your antivirus solution as certain changes can trick the antivirus and pose a risk for users. This book will help you to gain a basic understanding of antivirus software and take you through a series of antivirus bypass techniques that will enable you to bypass antivirus solutions. The book starts by introducing you to the cybersecurity landscape, focusing on cyber threats, malware, and more. You will learn how to collect leads to research antivirus and explore the two common bypass approaches used by the authors. Once you've covered the essentials of antivirus research and bypassing, you'll get hands-on with bypassing antivirus software using obfuscation, encryption, packing, PowerShell, and more. Toward the end, the book covers security improvement recommendations, useful for both antivirus vendors as well as for developers to help strengthen the security and malware detection capabilities of antivirus software. By the end of this security book, you'll have a better understanding of antivirus software and be able to confidently bypass antivirus software. What You Will Learn: Explore the security landscape and get to grips with the fundamentals of antivirus software Discover how to gather AV bypass research leads using malware analysis tools Understand the two commonly used antivirus bypass approaches Find out how to bypass static and dynamic antivirus engines Understand and implement bypass techniques in real-world scenarios Leverage best practices and recommendations for implementing antivirus solutions Who this book is for: This book is for security researchers, malware analysts, reverse engineers, pentesters, antivirus vendors looking to strengthen

their detection capabilities, antivirus users and companies that want to test and evaluate their antivirus software, organizations that want to test and evaluate antivirus software before purchase or acquisition, and tech-savvy individuals who want to learn new topics.

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.

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

Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building This book addresses topics in the area of forensic analysis of systems running on variants of the UNIX operating system, which is the choice of hackers for their attack platforms. According to a 2007 IDC report, UNIX servers account for the second-largest segment of spending (behind Windows) in the worldwide server market with $4.2 billion in 2Q07, representing 31.7% of corporate server spending. UNIX systems have not been analyzed to any significant depth largely due to a lack of understanding on the part of the investigator, an understanding and knowledge base that has been achieved by the attacker. The book begins with a chapter to describe why and how the book was written, and for whom, and then immediately begins addressing the issues of live response (volatile) data collection and analysis. The book continues by addressing issues of collecting and analyzing the contents of physical memory (i.e., RAM). The following chapters address /proc analysis, revealing the wealth of significant evidence, and analysis of files created by or on UNIX systems. Then the book addresses the underground world of UNIX hacking and reveals methods and techniques used by hackers, malware coders, and anti-forensic developers. The book then illustrates to the investigator how to analyze these files and extract the information they need to perform a comprehensive forensic analysis. The final chapter includes a detailed discussion of loadable kernel Modules and malware. Throughout the book the author provides a wealth of unique information, providing tools, techniques and information that won't be found anywhere else. This book contains information about UNIX forensic analysis that is not available anywhere else. Much of the information is a result of the author's own unique research

and work. The authors have the combined experience of law
enforcement, military, and corporate forensics. This unique
perspective makes this book attractive to all forensic
investigators.

"Incident Response is a complete guide for organizations of
all sizes and types who are addressing their computer
security issues."--Jacket.

Copyright: 8cc953e8d9af07183888d469653484aa