Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

Right here, we have countless ebook **Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches** and collections to check out. We additionally manage to pay for variant types and furthermore type of the books to browse. The pleasing book, fiction, history, novel, scientific research, as capably as various extra sorts of books are readily easy to use here.

As this Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches, it ends in the works creature one of the favored book Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches collections that we have. This is why you remain in the best website to see the unbelievable ebook to have.

FELIPE TRISTIAN

SQL Server Forensic Analysis Springer Nature This publication is intended to help organizations in investigating computer security incidents and troubleshooting some information technology (IT) operational problems by providing practical guidance on performing computer and network forensics. The guide presents forensics from an IT view, not a law enforcement view. Specifically, the publication describes the processes for performing effective forensics activities and provides advice regarding different data sources, including files, operating systems (OS), network traffic, and applications. The publication is not to be used as an allinclusivestep-by-step guide for executing a digital forensic investigation or construed as legal advice. Its purpose is to inform readers of various technologies and potential ways of using them in performing incident response or troubleshooting activities. Readers are advised to apply the recommended practices only after consulting

with management and legal counsel for compliance concerning laws and regulations (i.e., local, state, Federal, and international) that pertain to their situation. Incident Response Springer Nature 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 *Incident Response & Computer Forensics, Third Edition* Pearson Education OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset. Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations. Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator

are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones. Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately. For online source codes, please visit: https://github.com/jbradley89/osx_incident_response_scripting_and_analysis Focuses exclusively on OS X attacks, incident response, and forensics Provides the technical details of OS X so you can find artifacts that might be missed using automated tools

Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

Incident Response & Computer Forensics Createspace Independent Publishing Platform * Incident response and forensic investigation are the processes of detecting attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks * This much-needed reference covers the methodologies for incident response and computer forensics, Federal Computer Crime law information and evidence requirements, legal issues, and working with law enforcement * Details how to detect, collect, and eradicate breaches in e-mail and malicious code * CD-ROM is packed with useful tools that help capture and protect forensic data; search volumes, drives, and servers for evidence; and rebuild systems quickly after evidence has been obtained

Digital Forensics and Incident Response Syngress Develop the capacity to dig deeper into mobile device data acquisition About This Book A mastering guide to help you overcome the roadblocks you face when dealing with mobile forensics Excel at the art of extracting data, recovering deleted data, bypassing screen locks, and much more Get best practices to how to collect and analyze mobile device data and accurately document your investigations Who This Book Is For The book is for mobile forensics professionals who have experience in handling forensic tools and methods. This book is designed for skilled digital forensic examiners, mobile forensic investigators, and law enforcement officers. What You Will Learn Understand the mobile forensics process model and get guidelines on mobile device forensics Acquire in-depth knowledge about smartphone acquisition and acquisition methods Gain a solid understanding of the architecture of operating systems, file formats, and mobile phone internal memory Explore the topics of of mobile security, data leak, and evidence

recovery Dive into advanced topics such as GPS analysis, file carving, encryption, encoding, unpacking, and decompiling mobile application processes In Detail Mobile forensics presents a real challenge to the forensic community due to the fast and unstoppable changes in technology. This book aims to provide the forensic community an in-depth insight into mobile forensic techniques when it comes to deal with recent smartphones operating systems Starting with a brief overview of forensic strategies and investigation procedures, you will understand the concepts of file carving, GPS analysis, and string analyzing. You will also see the difference between encryption, encoding, and hashing methods and get to grips with the fundamentals of reverse code engineering. Next, the book will walk you through the iOS, Android and Windows Phone architectures and filesystem, followed by showing you various forensic approaches and data gathering techniques. You will also explore advanced forensic techniques and find out how to deal with third-applications using case studies. The book will help you master

data acquisition on Windows Phone 8. By the end of this book, you will be acquainted with best practices and the different models used in mobile forensics. Style and approach The book is a comprehensive guide that will help the IT forensics community to go more in-depth into the investigation process and mobile devices take-over.

Oracle Incident Response and Forensics

CRC Press

Organizations increasingly need to deal with unstructured processes that traditional business process management (BPM) suites are not designed to deal with. High-risk, yet high-value, loan origination or credit approvals, police investigations, and healthcare patient treatment are just a few examples of areas where a level of uncertainty makes outc

Computer Incident Response and Forensics Team Management

Springer Science & Business Media

Enhance your skills as a cloud investigator to adeptly respond to cloud incidents by combining traditional forensic techniques with innovative approaches Key Features Uncover the steps involved in cloud

forensic investigations for M365 and Google Workspace Explore tools and logs available within AWS, Azure, and Google for cloud investigations Learn how to investigate containerized services such as Kubernetes and Docker Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionAs organizations embrace cloud-centric environments, it becomes imperative for security professionals to master the skills of effective cloud investigation. Cloud Forensics Demystified addresses this pressing need, explaining how to use cloud-native tools and logs together with traditional digital forensic techniques for a thorough cloud investigation. The book begins by giving you an overview of cloud services, followed by a detailed exploration of the tools and techniques used to investigate popular cloud platforms such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). Progressing through the chapters, you'll learn how to investigate Microsoft 365, Google Workspace, and containerized environments such as Kubernetes. Throughout, the chapters emphasize the significance of the cloud, explaining which tools

and logs need to be enabled for investigative purposes and demonstrating how to integrate them with traditional digital forensic tools and techniques to respond to cloud security incidents. By the end of this book, you'll be well-equipped to handle security breaches in cloud-based environments and have a comprehensive understanding of the essential cloud-based logs vital to your investigations. This knowledge will enable you to swiftly acquire and scrutinize artifacts of interest in cloud security incidents. What you will learn Explore the essential tools and logs for your cloud investigation Master the overall incident response process and approach Familiarize yourself with the MITRE ATT&CK framework for the cloud Get to grips with live forensic analysis and threat hunting in the cloud Learn about cloud evidence acquisition for offline analysis Analyze compromised Kubernetes containers Employ automated tools to collect logs from M365 Who this book is for This book is for cybersecurity professionals, incident responders, and IT professionals adapting to the paradigm shift toward cloud-centric environments. Anyone

seeking a comprehensive guide to investigating security incidents in popular cloud platforms such as AWS, Azure, and GCP, as well as Microsoft 365, Google Workspace, and containerized environments like Kubernetes will find this book useful. Whether you're a seasoned professional or a newcomer to cloud security, this book offers insights and practical knowledge to enable you to handle and secure cloud-based infrastructure.

Incident Response & Computer Forensics, 2nd Edited, 2nd Edition

Packt Publishing Ltd

This book introduces and presents the newest up-to-date methods, approaches and technologies on how to detect child cyberbullying on social media as well as monitor kids E-learning, monitor games designed and social media activities for kids. On a daily basis, children are exposed to harmful content online. There have been many attempts to resolve this issue by conducting methods based on rating and ranking as well as reviewing comments to show the relevancy of these videos to children; unfortunately, there still remains a lack of supervision on videos

dedicated to kids. This book also introduces a new algorithm for content analysis against harmful information for kids. Furthermore, it establishes the goal to track useful information of kids and institutes detection of kid’s textual aggression through methods of machine and deep learning and natural language processing for a safer space for children on social media and online and to combat problems, such as lack of supervision, cyberbullying, kid’s exposure to harmful content. This book is beneficial to postgraduate students and researchers' concerns on recent methods and approaches to kids' cybersecurity.

Incident Response

Packt Publishing Ltd

Cyberforensics is a fairly new word in the technology our industry, but one that n- ertheless has immediately recognizable meaning. Although the word forensics may have its origins in formal debates using evidence, it is now most closely associated with investigation into evidence of crime. As the word cyber has become synonymous with the use of electronic technology, the word cyberforensics bears no mystery. It immediately conveys a serious and concentrated endeavor to

identify the evidence of crimes or other attacks committed in cyberspace. Nevertheless, the full implications of the word are less well understood. Cyberforensic activities remain a mystery to most people, even those fully immersed in the design and operation of cyber te- nology. This book sheds light on those activities in a way that is comprehensibl e not only to technology professionals but also to the technology hobbyist and those simply curious about the ?eld. When I started contributing to the ?eld of cybersecurity, it was an obscure ?eld, rarely mentioned in the mainstream media. According to the FBI, by 2009 organized crime syndicates were making more money via cybercrime than in drug traf?- ing. In spite of the rise in cybercrime and the advance of sophisticated threat actors online, the cyber security profession continues to lag behind in its ability to inves- gate cybercrime and understand the root causes of cyber attacks. In the late 1990s I worked to respond to sophisticated attacks as part of the U. S.

Learning Cyber Incident Response and Digital Forensics

5starcooks The tools and

techniques investigators need to conduct crucial forensic investigations in SQL Server. The database is the part of a forensic investigation that companies are the most concerned about. This book provides data and tools needed to avoid under or over reporting. Teaches many about aspects about SQL server that are not widely known. A complete tutorial to conducting SQL Server investigations and using that knowledge to confirm, assess, and investigate a digital intrusion. Companies today are in a terrible bind: They must report all possible data security breaches, but they don't always know if, in a given breech, data has been compromised. As a result, most companies are releasing information to the public about every system breech or attempted system breech they know about. This reporting, in turn, whips up public hysteria and makes many companies look bad. Kevvie Fowler's 'SQL Server Forensic Analysis' is an attempt to calm everyone down and focuses on a key, under-documented component of today's forensics investigations. The book will help investigators determine if a breech was attempted, if information on

the database server was compromised in any way, and if any rootkits have been installed that can compromise sensitive data in the future. Readers will learn how to prioritize, acquire, and analyze database evidence using forensically sound practices and free industry tools. The final chapter will include a case study that demonstrates all the techniques from the book applied in a walk-through of a real-world investigation.

Cyber Incident Response

Tata McGraw-Hill Education

Your in-depth guide to detecting network breaches, uncovering evidence, and preventing future attacks Whether it's from malicious code sent through an e-mail or an unauthorized user accessing company files, your network is vulnerable to attack. Your response to such incidents is critical. With this comprehensive guide, Douglas Schweitzer arms you with the tools to reveal a security breach, gather evidence to report the crime, and conduct audits to prevent future attacks. He also provides you with a firm understanding of the methodologies for incident response and computer forensics, Federal Computer Crime law information and evidence requirements, legal issues,

and how to work with law enforcement.

Guide to Integrating Forensic Techniques Into Incident Response

CRC Press

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. *Mastering Mobile Forensics* Newnes 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

Network Security Assessment

Syngress

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

Cloud Forensics Demystified

5starcooks

Operating System Forensics is the first book to cover all three critical operating systems for digital forensic investigations in one comprehensive reference. Users will learn how to conduct successful digital forensic examinations in Windows, Linux, and Mac OS, the methodologies used, key technical concepts, and the tools needed to perform examinations. Mobile operating systems such as Android,

iOS, Windows, and Blackberry are also covered, providing everything practitioners need to conduct a forensic investigation of the most commonly used operating systems, including technical details of how each operating system works and how to find artifacts. This book walks you through the critical components of investigation and operating system functionality, including file systems, data recovery, memory forensics, system configuration, Internet access, cloud computing, tracking artifacts, executable layouts, malware, and log files. You'll find coverage of key technical topics like Windows Registry, /etc directory, Web browers caches, Mbox, PST files, GPS data, ELF, and more. Hands-on exercises in each chapter drive home the concepts covered in the book. You'll get everything you need for a successful forensics examination, including incident response tactics and legal requirements. Operating System Forensics is the only place you'll find all this covered in one book.

Hands-on Incident Response and Digital Forensics

Packt Publishing Ltd

This timely text/reference

presents a detailed introduction to the essential aspects of computer network forensics. The book considers not only how to uncover information hidden in email messages, web pages and web servers, but also what this reveals about the functioning of the Internet and its core protocols. This, in turn, enables the identification of shortcomings and highlights where improvements can be made for a more secure network. Topics and features: provides learning objectives in every chapter, and review questions throughout the book to test understanding ; introduces the basic concepts of network process models, network forensics frameworks and network forensics tools; discusses various techniques for the acquisition of packets in a network forensics system, network forensics analysis, and attribution in network forensics; examines a range of advanced topics, including botnet, smartphone, and cloud forensics; reviews a number of freely available tools for performing forensic activities. Oracle Case Management Solutions Springer

How secure is your network? The best way to find out is to attack it, using the same tactics attackers employ to identify and exploit weaknesses. With the third edition of this practical book, you'll learn how to perform network-based penetration testing in a structured manner. Security expert Chris McNab demonstrates common vulnerabilities, and the steps you can take to identify them in your environment. System complexity and attack surfaces continue to grow. This book provides a process to help you mitigate risks posed to your network. Each chapter includes a checklist summarizing attacker techniques, along with effective countermeasures you can use immediately. Learn how to effectively test system components, including: Common services such as SSH, FTP, Kerberos, SNMP, and LDAP Microsoft services, including NetBIOS, SMB, RPC, and RDP SMTP, POP3, and IMAP email services IPsec and PPTP services that provide secure network access TLS protocols and features providing transport security Web server software, including Microsoft IIS, Apache, and Nginx Frameworks including

Rails, Django, Microsoft ASP.NET, and PHP Database servers, storage protocols, and distributed key-value stores

Computer Forensics

Rob Botwright

What are the disruptive Forensics and Incident Response technologies that enable your organization to radically change your business processes? What role does communication play in the success or failure of a Forensics and Incident Response project? What are your most important goals for the strategic Forensics and Incident Response objectives? Which individuals, teams or departments will be involved in Forensics and Incident Response? What would happen if Forensics and Incident Response weren't done? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to

ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Forensics and Incident Response investments work better. This Forensics and Incident Response All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Forensics and Incident Response Self-Assessment. Featuring 668 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Forensics and Incident Response improvements can be made. In using the questions you will be better able to: - diagnose Forensics and Incident Response projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement

evidence-based best practice strategies aligned with overall goals - integrate recent advances in Forensics and Incident Response and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Forensics and Incident Response Scorecard, you will develop a clear picture of which Forensics and Incident Response areas need attention. Your purchase includes access details to the Forensics and Incident Response self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard, and... - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation ...plus an extra, special, resource that helps you with project managing. INCLUDES LIFETIME SELF ASSESSMENT UPDATES

Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips. Computerworld Addison-Wesley Professional Computer forensics is the newest branch of computer security. This handbook provides useful guidance on the types of incidents, the legal and regulatory issues, and how to gather evidence that will stick in court.

OS X Incident Response Wiley 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 ...