

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

Provides an overview and case studies of computer crimes and discusses topics including data recovery, evidence collection, preservation of digital evidence, information warfare, and the cyber underground.

This is the only practical, hands-on guide available to database administrators to secure their Oracle databases. This book will help the DBA to assess their current level of risk as well as their existing security posture. It will then provide practical, applicable knowledge to appropriately secure the Oracle database. The only practical, hands-on guide for securing your Oracle database published by independent experts. Your Oracle database does not exist in a vacuum, so this book shows you how to securely integrate your database into your enterprise.

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

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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](http://www.mitre.org).

Computer Incident Response and Product Security

The practical guide to building and running incident response and product security teams Damir Rajnovic

Organizations increasingly recognize the urgent importance of effective, cohesive, and efficient security incident response. The speed and

effectiveness with which a company can respond to incidents has a direct impact on how devastating an incident is on the company's operations and finances. However, few have an experienced, mature incident response (IR) team. Many

companies have no IR teams at all; others need help with improving current practices. In this book,

leading Cisco incident response expert Damir Rajnović presents start-to-finish guidance for creating and operating effective IR teams and responding to incidents to lessen their impact significantly. Drawing on his extensive experience

identifying and resolving Cisco product security vulnerabilities, the author also covers the entire process of correcting product security vulnerabilities

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

and notifying customers. Throughout, he shows how to build the links across participants and processes that are crucial to an effective and timely response. This book is an indispensable resource for every professional and leader who must maintain the integrity of network operations and products—from network and security administrators to software engineers, and from product architects to senior security executives.

- Determine why and how to organize an incident response (IR) team
- Learn the key strategies for making the case to senior management
- Locate the IR team in your organizational hierarchy for maximum effectiveness
- Review best practices for managing attack situations with your IR team
- Build relationships with other IR teams, organizations, and law enforcement to improve incident response effectiveness
- Learn how to form, organize, and operate a product security team to deal with product vulnerabilities and assess their severity
- Recognize the differences between product security vulnerabilities and exploits
- Understand how to coordinate all the entities involved in product security handling
- Learn the steps for handling a product security vulnerability based on proven Cisco processes and practices
- Learn strategies for notifying customers about product vulnerabilities and how to ensure customers are implementing fixes

This security book is part of the Cisco Press Networking Technology Series.

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end, self-defending networks.

Updated with the latest advances from the field, **GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS**, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the tools and techniques of the trade, it introduces readers to every step of the computer forensics investigation-from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

**Windows Registry Forensics** provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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

Written by FBI insiders, this updated best-seller offers a look at the legal, procedural, and technical steps of incident response and computer forensics. Including new chapters on forensic analysis and remediation, and real-world case studies, this revealing book shows how to counteract and

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

conquer today's hack attacks.

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.

Cyberforensics is a fairly new word in the technology our industry, but one that nevertheless 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 technology. This book sheds light on those activities in a way that is comprehensible not only to technology professionals but also to the technology hobbyist and those simply curious about the field. When I started contributing to the field of

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

cybersecurity, it was an obscure field, rarely mentioned in the mainstream media. According to the FBI, by 2009 organized crime syndicates were making more money via cybercrime than in drug trafficking. 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 investigate 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.

An incident management and response guide for IT or security professionals wanting to establish or improve their incident response and overall security capabilities. Included are templates for response tools, policies, and plans. This look into how to plan, prepare, and respond also includes links to valuable resources needed for planning, training, and overall management of a Computer Security Incident Response Team.

Auditing is constantly and quickly changing due to the continuous evolution of information and communication technologies. As the auditing process is forced to adapt to these changes, issues have arisen that lead to a decrease in the auditing effectiveness and efficiency, leading to a greater dissatisfaction among users. More research is needed to provide effective management and mitigation of the risk associated to organizational

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

transactions and to assign a more reliable and accurate character to the execution of business transactions and processes. Organizational Auditing and Assurance in the Digital Age is an essential reference source that discusses challenges, identifies opportunities, and presents solutions in relation to issues in auditing, information systems auditing, and assurance services and provides best practices for ensuring accountability, accuracy, and transparency. Featuring research on topics such as forensic auditing, financial services, and corporate governance, this book is ideally designed for internal and external auditors, assurance providers, managers, risk managers, academicians, professionals, and students.

Cybersecurity and Privacy in Cyber-Physical Systems collects and reports on recent high-quality research that addresses different problems related to cybersecurity and privacy in cyber-physical systems (CPSs). It Presents high-quality contributions addressing related theoretical and practical aspects Improves the reader's awareness of cybersecurity and privacy in CPSs Analyzes and presents the state of the art of CPSs, cybersecurity, and related technologies and methodologies Highlights and discusses recent developments and emerging trends in cybersecurity and privacy in CPSs Proposes new models, practical solutions, and technological advances related to cybersecurity and privacy in



## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

CPSs Discusses new cybersecurity and privacy models, prototypes, and protocols for CPSs This comprehensive book promotes high-quality research by bringing together researchers and experts in CPS security and privacy from around the world to share their knowledge of the different aspects of CPS security. *Cybersecurity and Privacy in Cyber-Physical Systems* is ideally suited for policymakers, industrial engineers, researchers, academics, and professionals seeking a thorough understanding of the principles of cybersecurity and privacy in CPSs. They will learn about promising solutions to these research problems and identify unresolved and challenging problems for their own research. Readers will also have an overview of CPS cybersecurity and privacy design.

**PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition** presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

**OS X Incident Response: Scripting and Analysis is**

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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](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

From operating systems to the cloud, Oracle's products and services are everywhere, and it has the market share to prove it. Given the share diversity of the Oracle product line, and the level of complexity of integration, management can be quite a daunting task. The CIO's Guide to Oracle Products and Solutions is the go-to guide for all things Oracle. If you are a typical Oracle professional, you don't have the luxury of time to keep up with new technology and read all the new manuals to understand each new feature of the latest release from Oracle. You need a comprehensive source of

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

information and in-depth tips and techniques for using the new technology. You need Oracle Internals: Tips, Trick

Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treacherous 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

Incident response is a multidisciplinary science that resolves computer crime and complex legal issues, chronological methodologies and technical computer techniques. The commercial industry has embraced and adopted technology that detects hacker incidents. Companies are swamped with real attacks, yet very few have any methodology or knowledge to resolve these attacks. Incident Response: Investigating Computer Crime will be the only book on the market that provides the information on incident response that network professionals need to conquer attacks.

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

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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

The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book. An example-driven approach to securing Oracle APEX applications As a Rapid Application Development framework, Oracle Application Express (APEX) allows websites to easily be created based on data within an Oracle database. Using only a web browser, you can develop and deploy professional applications that are both fast and secure. However, as with any website, there is a security risk and threat, and securing APEX applications requires some specific knowledge of the framework. Written by well-known security specialists Recx, this book shows you the correct ways to implement your APEX applications to ensure that they are not vulnerable to attacks. Real-world examples of a variety of security vulnerabilities demonstrate attacks and show the techniques and best practices for making applications secure.

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

Divides coverage into four sections, three of which cover the main classes of threat faced by web applications and the fourth covers an APEX-specific protection mechanism. Addresses the security issues that can arise, demonstrating secure application design. Examines the most common class of vulnerability that allows attackers to invoke actions on behalf of other users and access sensitive data. The lead-by-example approach featured in this critical book teaches you basic "hacker" skills in order to show you how to validate and secure your APEX applications. 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 breach, data has been compromised. As a result, most companies are releasing information to the public about every system breach or attempted system breach 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 breach 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

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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.

Oracle Incident Response and Forensics Preparing for and Responding to Data Breaches Apress

Complex problems and systems, which prevail in the real world, cannot often be tackled and solved either by traditional methods offered by mathematics or even the traditional computer science (CS) and artificial intelligence (AI)..).

What is the way out of this dilemma? Advanced methodologies, and tools and techniques, mimicking human reasoning or the behavior of animals, animal populations or certain parts of the living bod, based on traditional computer science science and the initial approaches of artificial intelligence are often referred to as biologically inspired methods, or often computational intelligence (CI).

Computational intelligence offers effective and efficient solutions to many unsolvable" problems problems. However, it is far from being a ready to use and complete collection of approaches, and is rather a continuously developing field without clear borders. The emerging new models and algorithms of computational intelligence are deeply rooted in the vast apparatus of traditional mathematics. Thus, the investigation of connections and synergy between mathematics and computational intelligence is an eminent goal which is periodically pursued by a group of mathematicians and computational intelligence researchers who regularly attend the annual European Symposia on Computational Intelligence and Mathematics (ESCIM). Some relevant papers from the last ESCIM-2020 are included in this volume.

**A Practical Guide to Computer Forensics Investigations** introduces the newest technologies

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

along with detailed information on how the evidence contained on these devices should be analyzed. Packed with practical, hands-on activities, students will learn unique subjects from chapters including Mac Forensics, Mobile Forensics, Cyberbullying, and Child Endangerment. This well-developed book will prepare students for the rapidly-growing field of computer forensics for a career with law enforcement, accounting firms, banks and credit card companies, private investigation companies, or government agencies.

This book is an anthology of effective database management techniques representing the collective wisdom of the OakTable Network. With an emphasis upon performance—but also branching into security, national language, and other issues—the book helps you deliver the most value for your company's investment in Oracle Database technologies. You'll learn to effectively plan for and monitor performance, to troubleshoot systematically when things go wrong, and to manage your database rather than letting it manage you.

\* Prepares readers for the Certified Information Security Manager (CISM) exam, ISACA's new certification that launches in June 2003 \* CISM is business-oriented and intended for the individual who must manage, design, oversee, and assess an enterprise's information security \* Essential reading for those who are cramming for this new test and



## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

need an authoritative study guide \* Many out-of-work IT professionals are seeking security management certification as a vehicle to re-employment \* CD-ROM includes a Boson-powered test engine with all the questions and answers from the book

Protecting Oracle Database 12c helps you solve the problem of maximizing the safety, resilience, and security of an Oracle database whilst preserving performance, availability, and integration despite ongoing and new security issues in the software. The book demonstrates, through coded examples, how you can enable the consolidation features of Oracle Database 12c without increasing risk of either internal corruption or external vulnerability. In addition, new protections not publicly available are included, so that you can see how demonstrable risk improvements can be achieved, measured, and reported through Enterprise Manager 12c. Most importantly, the challenge of privileged access control within a consolidation environment will be addressed, thus enabling a safe move to greater efficiency.

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

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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.

This guide teaches security analysts to minimize information loss and system disruption using effective system monitoring and detection measures. The information here spans all phases of incident response, from pre-incident conditions and considerations to post-incident analysis. This book will deliver immediate solutions to a growing audience eager to secure its networks.

Launch Your Career in Computer Forensics—Quickly and Effectively Written by a team of computer forensics experts, Computer Forensics JumpStart provides all the core information you need to launch your career in this fast-growing field: Conducting a computer forensics investigation Examining the layout of a network Finding hidden data Capturing

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

images Identifying, collecting, and preserving  
computer evidence Understanding encryption and  
examining encrypted files Documenting your case  
Evaluating common computer forensic tools  
Presenting computer evidence in court as an expert  
witness

Take the right steps when a breach of your Oracle  
Database environment becomes known or  
suspected. You will learn techniques for discerning  
how an attacker got in, what data they saw, and  
what else they might have done. This book helps  
you understand forensics in relation to Oracle  
Database, and the tools and techniques that should  
be used to investigate a database breach. You will  
learn the measures to put in place now to make it  
harder for an attack to be successful, and to aid in  
the detection and investigation of future attacks. You  
will know how to bring together tools and methods to  
create a holistic approach and investigation when an  
event occurs, helping you to be confident of your  
ability to react correctly and responsibly to threats  
against your organization's data. What You'll Learn  
Detect when breaches have or may have occurred  
React with confidence using an organized plan  
Determine whether a suspected breach is real  
Determine the scope of data that has been  
compromised Preserve evidence for possible  
criminal prosecutions Put in place measures to aid  
future investigations Who This Book is For Database

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

administrators, system administrators, and other technology professionals who may be called upon to investigate breaches of security involving Oracle Database

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

When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm. What's the worst

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antifoensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle. Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability. Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands. "Incident Response is a complete guide for organizations of all sizes and types who are addressing their computer security issues."--Jacket.

Implement a robust SIEM system Effectively manage the security information and events produced by your network with help from this authoritative guide. Written

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

by IT security experts, Security Information and Event Management (SIEM) Implementation shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You'll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource. Assess your organization's business models, threat models, and regulatory compliance requirements Determine the necessary SIEM components for small- and medium-size businesses Understand SIEM anatomy—source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring Develop an effective incident response program Use the inherent capabilities of your SIEM system for business intelligence Develop filters and correlated event rules to reduce false-positive alerts Implement AlienVault's Open Source Security Information Management (OSSIM) Deploy the Cisco Monitoring Analysis and Response System (MARS) Configure and use the Q1 Labs QRadar SIEM system Implement ArcSight Enterprise Security Management (ESM) v4.5 Develop your SIEM security analyst skills When you need practical hands-on support for Active Directory, the updated edition of this extremely popular Cookbook provides quick solutions to more than 300 common (and uncommon) problems you might encounter when deploying, administering, and automating Microsoft's network directory service. For the

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

third edition, Active Directory expert Laura E. Hunter offers troubleshooting recipes based on valuable input from Windows administrators, in addition to her own experience. You'll find solutions for the Lightweight Directory Access Protocol (LDAP), ADAM (Active Directory Application Mode), multi-master replication, Domain Name System (DNS), Group Policy, the Active Directory Schema, and many other features. The Active Directory Cookbook will help you:

- Perform Active Directory tasks from the command line
- Use scripting technologies to automate Active Directory tasks
- Manage new Active Directory features, such as Read-Only Domain Controllers, fine-grained password policies, and more
- Create domains and trusts
- Locate users whose passwords are about to expire
- Apply a security filter to group policy objects
- Check for potential replication problems
- Restrict hosts from performing LDAP queries
- View DNS server performance statistics

Each recipe includes a discussion explaining how and why the solution works, so you can adapt the problem-solving techniques to similar situations. Active Directory Cookbook is ideal for any IT professional using Windows Server 2008, Exchange 2007, and Identity Lifecycle Manager 2007, including Active Directory administrators looking to automate task-based solutions. "It is rare for me to visit a customer site and not see a copy of Active Directory Cookbook on a shelf somewhere, which is a testament to its usefulness. The Cookbook takes the pain out of everyday AD tasks by providing concise, clear and relevant recipes. The fact that the recipes are provided using different methods (graphical user



## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

interface, command line and scripting) means that the book is suitable for anyone working with AD on a day-to-day basis. The introduction of PowerShell examples in this latest edition will be of particular interest for those looking to transition from VBScript. Laura has also done a great job in extending the Cookbook in this edition to encompass the broad range of changes to AD in Windows Server 2008." --Tony Murray, Founder of Activedir.org and Directory Services MVP "If you already understand Active Directory fundamentals and are looking for a quick solution to common Active Directory related tasks, look no further, you have found the book that you need." --Joe Richards, Directory Services MVP "The Active Directory Cookbook is the real deal... a soup-to-nuts catalog of every administrative task an Active Directory administrator needs to perform. If you administer an Active Directory installation, this is the very first book you have to put on your shelf." --Gil Kirkpatrick, Chief Architect, Active Directory and Identity Management, Quest Software and Directory Services MVP

This book is about database security and auditing. You will learn many methods and techniques that will be helpful in securing, monitoring and auditing database environments. It covers diverse topics that include all aspects of database security and auditing - including network security for databases, authentication and authorization issues, links and replication, database Trojans, etc. You will also learn of vulnerabilities and attacks that exist within various database environments or that have been used to attack databases (and that

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

have since been fixed). These will often be explained to an “internals level. There are many sections which outline the “anatomy of an attack – before delving into the details of how to combat such an attack. Equally important, you will learn about the database auditing landscape – both from a business and regulatory requirements perspective as well as from a technical implementation perspective. \* Useful to the database administrator and/or security administrator - regardless of the precise database vendor (or vendors) that you are using within your organization. \* Has a large number of examples - examples that pertain to Oracle, SQL Server, DB2, Sybase and even MySQL.. \* Many of the techniques you will see in this book will never be described in a manual or a book that is devoted to a certain database product. \* Addressing complex issues must take into account more than just the database and focusing on capabilities that are provided only by the database vendor is not always enough. This book offers a broader view of the database environment - which is not dependent on the database platform - a view that is important to ensure good database security.

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

## Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

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.

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, *What Every Engineer Should Know About Cyber Security and Digital Forensics* is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to

# Get Free Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

break into this expanding profession.

[Copyright: 985e8f873d9022fe4ae2207abfbb58ee](#)