

Windows Logon Forensics Sans Institute

The first book completely devoted to this important part of security in a Windows environment. An authoritative guide to investigating high-technology crimes Internet crime is seemingly ever on the rise, making the need for a comprehensive resource on how to investigate these crimes even more dire. This professional-level book--aimed at law enforcement personnel, prosecutors, and corporate investigators--provides you with the training you need in order to acquire the sophisticated skills and software solutions to stay one step ahead of computer criminals. Specifies the techniques needed to investigate, analyze, and document a criminal act on a Windows computer or network Places a special emphasis on how to thoroughly investigate criminal activity and now just perform the initial response Walks you through ways to present technically complicated material in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 and Windows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academic adoption, Mastering Windows Network Forensics and Investigation, 2nd Edition offers help for investigating high-technology crimes.

Download Ebook Windows Logon Forensics Sans Institute

??C???

This work introduces the reader to the world of digital forensics in a practical and accessible manner. The text was written to fulfill a need for a book that introduces forensic methodology and sound forensic thinking, combined with hands-on examples for common tasks in a computer forensic examination. The author has several years of experience as a computer forensics examiner and is now working as a university-level lecturer. Guide to Digital Forensics: A Concise and Practical Introduction is intended for students that are looking for an introduction to computer forensics and can also be used as a collection of instructions for practitioners. The aim is to describe and explain the steps taken during a forensic examination, with the intent of making the reader aware of the constraints and considerations that apply during a forensic examination in law enforcement and in the private sector. Upon reading this book, the reader should have a proper overview of the field of digital forensics, starting them on the journey of becoming a computer forensics expert. Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey brings together a few top experts to create the first detailed guide for professionals who are already familiar with digital evidence. The Handbook of Computer Crime Investigation helps readers

Download Ebook Windows Logon Forensics Sans Institute

master the forensic analysis of computer systems with a three-part approach covering tools, technology, and case studies. The Tools section provides the details on leading software programs, with each chapter written by that product's creator. The section ends with an objective comparison of the strengths and limitations of each tool. The main Technology section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, moving on to networks, and culminating with embedded systems. The Case Examples section gives readers a sense of the technical, legal, and practical challenges that arise in real computer investigations. The Tools section provides details of leading hardware and software The main Technology section provides the technical "how to" information for collecting and analysing digital evidence in common situations Case Examples give readers a sense of the technical, legal, and practical challenges that arise in real computer investigations 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

Download Ebook Windows Logon Forensics Sans Institute

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

Presents information on security Apache Web servers and Web applications.

????????????,????Windows????????????,?????Windows?????
????????????????????????????,?????Windows????????????????
????????,??Rootkits????
????????????????????????,????????????????,????????????????????????

Download Ebook Windows Logon Forensics Sans Institute

??????,??????????????????????.

?????????????????Mark Russinovich?David Solomon???Windo
ws??????????????,??????????Windows??????????????????????

Dissecting the Hack: The F0rb1dd3n Network, Revised Edition, deals with hackers and hacking. The book is divided into two parts. The first part, entitled “The F0rb1dd3n Network, tells the fictional story of Bob and Leon, two kids caught up in an adventure where they learn the real-world consequence of digital actions. The second part, “Security Threats Are Real (STAR), focuses on these real-world lessons. The F0rb1dd3n Network can be read as a stand-alone story or as an illustration of the issues described in STAR. Throughout The F0rb1dd3n Network are “Easter eggs —references, hints, phrases, and more that will lead readers to insights into hacker culture. Drawing on The F0rb1dd3n Network, STAR explains the various aspects of reconnaissance; the scanning phase of an attack; the attacker’s search for network weaknesses and vulnerabilities to exploit; the various angles of attack used by the characters in the story; basic methods of erasing information and obscuring an attacker’s presence on a computer system; and the underlying hacking culture. Revised edition includes a completely NEW STAR Section (Part 2) Utilizes actual hacking and security tools in its story- helps to familiarize a newbie with the many devices and their code Introduces basic hacking techniques in real life context for ease of learning

?????????????????????.???19?,?1????????????;?2????????????;?3??
????????????;?4????????????;?5????????????????;?6????????????????;
?7????????????????;?8????????????;?9????????????;?10????????????;?1
1???Windows????????;?12???UNIX?Linux????????;?13????????????;
?14???PKI????????;?15????????????????;?16????????????????????;?17???
????????????????;?18????????????????;?19?????????????.

* Incident response and forensic investigation are the

Download Ebook Windows Logon Forensics Sans Institute

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
?????????Reporting Services?????,?????????,?????????????
???,?????????????????
????16?,??:“?????”?“?????”?“?????”?“?????”?“?????”
?????”??

This book contains a selection of thoroughly refereed and revised papers from the Third International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2011, held October 26-28 in Dublin, Ireland. The field of digital forensics is becoming increasingly important for law enforcement, network security, and information assurance. It is a multidisciplinary area that encompasses a number of fields, including law, computer science, finance, networking, data mining, and criminal justice. The 24 papers in this volume cover a variety of topics ranging from tactics of cyber crime investigations to digital forensic education, network forensics, and the use of formal methods in digital investigations. There is a large section addressing forensics of mobile digital devices.

TICSA (TruSecure ICSA Computer Security Associate) is an entry-level computer security certification aimed at individuals with one to three years of computer security experience. TICSA represents base level certification, and is designed for network administrators responsible for security administration

Download Ebook Windows Logon Forensics Sans Institute

of systems or networks in an enterprise.

The second edition of this comprehensive handbook of computer and information security provides the most complete view of computer security and privacy available. It offers in-depth coverage of security theory, technology, and practice as they relate to established technologies as well as recent advances. It explores practical solutions to many security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. The book is organized into 10 parts comprised of 70 contributed chapters by leading experts in the areas of networking and systems security, information management, cyber warfare and security, encryption technology, privacy, data storage, physical security, and a host of advanced security topics. New to this edition are chapters on intrusion detection, securing the cloud, securing web apps, ethical hacking, cyber forensics, physical security, disaster recovery, cyber attack deterrence, and more. Chapters by leaders in the field on theory and practice of computer and information security technology, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

??
??

PART OF THE NEW JONES & BARTLETT LEARNING
INFORMATION SYSTEMS SECURITY & ASSURANCE
SERIES Completely revised and rewritten to keep pace with
the fast-paced field of Computer Forensics! Computer crimes
call for forensics specialists, people who know how to find

Download Ebook Windows Logon Forensics Sans Institute

and follow the evidence. System Forensics, Investigation, and Response, Second Edition begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. New and Key Features of the Second Edition: Examines the fundamentals of system forensics Discusses computer crimes and forensic methods Written in an accessible and engaging style Incorporates real-world examples and engaging cases Instructor Materials for System Forensics, Investigation, and Response include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts Instructor's Manual

????????????

?????:????

????????????,????????????C++????????,????????????,?
????????????????????????????,????????????????,????????????
??

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

Download Ebook Windows Logon Forensics Sans Institute

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

107, : SQL Server SQL Server
Server
Server, ,
Server

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write

Download Ebook Windows Logon Forensics Sans Institute

Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

"Cybercrime and cyber-terrorism represent a serious challenge to society as a whole." - Hans Christian Krüger, Deputy Secretary General of the Council of Europe Crime has been with us as long as laws have existed, and modern technology has given us a new type of criminal activity: cybercrime. Computer and network related crime is a problem that spans the globe, and unites those in two disparate fields: law enforcement and information technology. This book will help both IT pros and law enforcement specialists understand both their own roles and those of the other, and show why that understanding and an organized, cooperative effort is necessary to win the fight against this new type of crime.

62% of US companies reported computer-related security breaches resulting in damages of \$124 million dollars. This data is an indication of the massive need for Cybercrime training within the IT and law enforcement communities. The only book that covers Cybercrime from forensic investigation through prosecution. Cybercrime is one of the battlefields in the war against terror.

????????????????,???UNIX???C????????????,??????????
????????????IT????????????UNIX????????????

Fourth Edition (Traditional Chinese Translation)
Sheds New Light on Open Source Intelligence
Collection and Analysis. Author Michael Bazzell has

Download Ebook Windows Logon Forensics Sans Institute

been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Owner Information Twitter GPS & Account Data Hidden Photo GPS & Metadata Deleted Websites & Posts Website Owner Information Alias Social Network Profiles Additional User Accounts Sensitive Documents & Photos Live Streaming Social Content

Download Ebook Windows Logon Forensics Sans Institute

IP Addresses of Users Newspaper Archives & Scans
Social Content by Location Private Email Addresses
Hidden Personal Videos Duplicate Copies of Photos
Personal Radio Communications Compromised
Email Information Wireless Routers by Location
Hidden Mapping Applications Complete Facebook
Data Free Investigative Software Alternative Search
Engines Mobile App Network Data Unlisted
Addresses Unlisted Phone Numbers Useful Browser
Extensions Public Government Records Document
Metadata Rental Vehicle Contracts Online Criminal
Activity

????

????????Linux????????????,????????????????????,?

????????Intel????????

[Copyright: 6fcf7832820ccd8f8ae2e408a5066dc7](https://www.sans.org/whitepapers/windows-logon-forensics)