

Microsoft Log Parser Toolkit A Complete Toolkit For Microsofts Undocumented Log Analysis Tool

Microsoft Operations Manager (MOM) is a network monitoring tool that provides enterprise-class event and performance management for Windows Server System technologies. MOM's event and performance management tools discover problems before system administrators would ever find them, thereby enabling administrators to lower their costs of operations and simplify management of their Windows Server System infrastructure. MOM can notify system administrators of overloaded processors, depleted memory, or failed network connections affecting their Windows servers long before these problems bother users. Microsoft Operations Manager (MOM) 2005 delivers open and scalable enterprise-class operational management by providing comprehensive event management, proactive monitoring and alerting, reporting and trend analysis, and system and application specific knowledge and tasks to improve the manageability of Windows Server System environments, including Windows, Exchange, SQL, IIS, Active Directory etc. * A users guide to Microsoft Operations Manager (MOM) enabling a cost reduction and simplification in managing your Windows Server System Infrastructure * Companion Web site for book offers dozens of customized scripts and tools for automating MOM 2005 and many other Windows Server products * There is no other compact resource like this for this core, Microsoft Server product

This book will detail the default and custom installation of VMware's ESx server as well as basic and advanced virtual machine configurations. It will also discuss the requirements for a server virtualization and consolidation project and the cost savings surrounding such an effort. Furthermore, the book will provide a thorough understanding of the benefits of a virtual infrastructure and a comprehensive examination of how VMware eases administration and lowers overall IT costs. Lastly, the book delivers a thorough understanding of the virtual evolution which is underway in many IT organizations and how the reader will benefit from shifting from the physical to a virtual * A detailed resource on the default and custom installation of VMware's ESx server * Covers all the requirements for a server virtualization and consolidation project and the cost savings surrounding such an effort * Delivers a thorough understanding of the virtual evolution occurring in the IT industry

A C# developer's book and eBook guide to the features and programming interfaces of Windows Workflow Foundation. According to the Brookings Institute, an organization's information and other intangible assets account for over 80 percent of its market value. As the primary sponsors and implementers of information security programs, it is essential for those in key leadership positions to possess a solid understanding of the constantly evolving fundamental concepts of information security. 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

This book teaches IT professionals how to analyze, manage, and automate their security log files to generate useful, repeatable information that can be used to make their networks more efficient and secure using primarily open source tools. The book begins by discussing the "Top 10 security logs that every IT professional should be regularly analyzing. These 10 logs cover everything from the top workstations sending/receiving data through a firewall to the top targets of IDS alerts. The book then goes on to discuss the relevancy of all of this information. Next, the book describes how to script open source reporting tools like Tcpsdstats to automatically correlate log files from the various network devices to the "Top 10 list. By doing so, the IT professional is instantly made aware of any critical vulnerabilities or serious degradation of network performance. All of the scripts presented within the book will be available for download from the Syngress Solutions Web site. Almost every operating system, firewall, router, switch, intrusion detection system, mail server, Web server, and database produces some type of "log file. This is true of both open source tools and commercial software and hardware from every IT manufacturer. Each of these logs is reviewed and analyzed by a system administrator or security professional responsible for that particular piece of hardware or software. As a result, almost everyone involved in the IT industry works with log files in some capacity. * Provides turn-key, inexpensive, open source solutions for system administrators to analyze and evaluate the overall performance and security of their network * Dozens of working scripts and tools presented throughout the book are available for download from Syngress Solutions Web site. * Will save system administrators countless hours by scripting and automating the most common to the most complex log analysis tasks

User passwords are the keys to the network kingdom, yet most users choose overly simplistic passwords (like password) that anyone could guess, while system administrators demand impossible to remember passwords littered with obscure characters and random numerals. Every computer user must face the problems of password security. According to a recent British study, passwords are usually obvious: around 50 percent of computer users select passwords based on names of a family member, spouse, partner, or a pet. Many users face the problem of selecting strong passwords that meet corporate security requirements. Too often, systems reject user-selected passwords because they are not long enough or otherwise do not meet complexity requirements. This book teaches users how to select passwords that always meet complexity requirements. A typical computer user must remember dozens of passwords and they are told to make them all unique and never write them down. For most users, the solution is easy passwords that follow simple patterns. This book teaches users how to select strong passwords they can easily remember. * Examines the password problem from the perspective of the administrator trying to secure their network * Author Mark Burnett has accumulated and

analyzed over 1,000,000 user passwords and through his research has discovered what works, what doesn't work, and how many people probably have dogs named Spot * Throughout the book, Burnett sprinkles interesting and humorous password ranging from the Top 20 dog names to the number of references to the King James Bible in passwords This book includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Computer Science, Computer Engineering and Information Sciences. The book presents selected papers from the conference proceedings of the International Conference on Systems, Computing Sciences and Software Engineering (SCSS 2006). All aspects of the conference were managed on-line.

How to Cheat at Windows Systems Administrators using Command Line Scripts teaches system administrators hundreds of powerful, time-saving tips for automating daily system administration tasks using Windows command line scripts. With every new version of Windows, Microsoft is trying to ease the administration jobs by adding more and more layers of graphical user interface (GUI) or configuration wizards (dialog boxes). While these 'wizards' are interactive and make the administrator's job easier, they are not always the most convenient and efficient way to accomplish the everyday administration tasks. These wizards are time consuming and, at times, may seem a bit confusing. The purpose of the book is to teach administrators how to use command-line scripts to complete everyday administration jobs, solve recurring network problems and at the same time improve their efficiency. Provides system administrators with hundreds of tips, tricks, and scripts to complete administration tasks more quickly and efficiently. No direct competition for a core tool for Windows administrators. Builds on success of other books in the series including How to Cheat at Managing Windows Small Business Server 2003 and How to Cheat at Managing Microsoft Operations Manager 2005.

In order to establish and then maintain a successful presence on the Web, designing a creative site is only half the battle. What good is an intricate Web infrastructure if you're unable to measure its effectiveness? That's why every business is desperate for feedback on their site's visitors: Who are they? Why do they visit? What information or service is most valuable to them? Unfortunately, most common Web analytics software applications are long on functionality and short on documentation. Without clear guidance on how these applications should be integrated into the greater Web strategy, these often expensive investments go underused and underappreciated. Enter Web Site Measurement Hacks, a guidebook that helps you understand your Web site visitors and how they contribute to your business's success. It helps organizations and individual operators alike make the most of their Web investment by providing tools, techniques, and strategies for measuring--and then improving--their site's usability, performance, and design. Among the many topics covered, you'll learn: definitions of commonly used terms, such as "key performance indicators" (KPIs) how to drive potential customers to action how to gather crucial marketing and customer data which features are useful and which are superfluous advanced techniques that senior Web site analysts use on a daily basis By examining how real-world companies use analytics to their success, Web Site Measurement Hacks demonstrates how you, too, can accurately measure your Web site's overall effectiveness. Just as importantly, it bridges the gulf between the technical teams charged with maintaining your Web's infrastructure and the business teams charged with making management decisions. It's the technology companion that every site administrator needs.

Pro Exchange Server 2013 Administration is your best-in-class companion for gaining a deep, thorough understanding of Microsoft's powerful enterprise collaboration and communications server. Author Jaap Wesselius is at your side as you administer every facet of Exchange Server 2013, revealing tips, tricks, and little known facts that will make your administration life simpler and more effective. Along with revealing what's new in Exchange Server 2013, this well-paced, deeply engaging tutorial provides detailed deployment guidance, for upgraders and migrators as well as for organizations entirely new to the Exchange platform. The book details how all of the major Exchange components fit together, from SMTP messages to all kinds of clients. It also provides in-depth configuration examples with an eye toward creating scalable, reliable, and secure installations. Additionally, this guide covers the tools and techniques for monitoring an Exchange environment and troubleshooting when things go wrong. With Pro Exchange Server 2013 Administration, you will:

- Learn how to install Exchange Server fresh or upgrade from a previous version
- Get a comprehensive understanding of Exchange, with thorough coverage of Mailbox server and Client Access server
- Understand the tools and techniques for configuring and managing your Exchange deployment to ensure scalability, reliability, efficiency and security
- Learn how to monitor your deployment and prepare for any problems and how to troubleshoot any problems that do arise

CompTIA Security+ Certification Study Guide: Exam SYO-201, Third Edition, offers a practical guide for those interested in pursuing CompTIA Security+ certification. The book is organized into six parts. Part 1 deals with general security issues including security threats; hardware and peripheral security risks; the fundamentals of operating system (OS) hardening; implementing system security applications; and concepts of virtualization. Part 2 discusses the fundamentals of network security. Part 3 focuses on network access and network authentication. Part 4 explains the importance of risk assessments and risk mitigation, and how to conduct them. Part 5 reviews general cryptographic concepts and addresses the complex issues involved in planning a certificate-based public key infrastructure (PKI). Part 6 on organizational security discusses redundancy planning; environmental controls; implementing disaster recovery and incident response procedures; and the policies, procedures, and documentation upon which organizational computer security is based. Each chapter begins with Exam Objectives and concludes with Self-Test questions along with their corresponding answers. *Complete exam-prep package includes full coverage of new Security+ objectives, flash cards, cram sheets, MP3s for exam-day study, PPT presentations, two complete practice exams, and certification e-book library *Authored by a leading Microsoft security expert *A good reference for both beginning security professionals and seasoned IT professionals

* Task-based, advanced solutions * Discusses non-traditional or out-of-band solutions * Written from real-world

knowledge * Focuses on solutions relevant to consultants

The Programmer's Ultimate Security DeskRef is the only complete desk reference covering multiple languages and their inherent security issues. It will serve as the programming encyclopedia for almost every major language in use. While there are many books starting to address the broad subject of security best practices within the software development lifecycle, none has yet to address the overarching technical problems of incorrect function usage. Most books fail to draw the line from covering best practices security principles to actual code implementation. This book bridges that gap and covers the most popular programming languages such as Java, Perl, C++, C#, and Visual Basic. * Defines the programming flaws within the top 15 programming languages. * Comprehensive approach means you only need this book to ensure an application's overall security. * One book geared toward many languages.

The book covers a decade of work with some of the largest commercial and government agencies around the world in addressing cyber security related to malicious insiders (trusted employees, contractors, and partners). It explores organized crime, terrorist threats, and hackers. It addresses the steps organizations must take to address insider threats at a people, process, and technology level. Today's headlines are littered with news of identity thieves, organized cyber criminals, corporate espionage, nation-state threats, and terrorists. They represent the next wave of security threats but still possess nowhere near the devastating potential of the most insidious threat: the insider. This is not the bored 16-year-old hacker. We are talking about insiders like you and me, trusted employees with access to information - consultants, contractors, partners, visitors, vendors, and cleaning crews. Anyone in an organization's building or networks that possesses some level of trust. * Full coverage of this hot topic for virtually every global 5000 organization, government agency, and individual interested in security. * Brian Contos is the Chief Security Officer for one of the most well known, profitable and respected security software companies in the U.S.—ArcSight.

This comprehensive guide provides you with the training you need to arm yourself against phishing, bank fraud, unlawful hacking, and other computer crimes. Two seasoned law enforcement professionals discuss everything from recognizing high-tech criminal activity and collecting evidence to presenting it in a way that judges and juries can understand. They cover the range of skills, standards, and step-by-step procedures you'll need to conduct a criminal investigation in a Windows environment and make your evidence stand up in court.

Most Systems Administrators are not security specialists. Keeping the network secure is one of many responsibilities, and it is usually not a priority until disaster strikes. How to Cheat at Securing Your Network is the perfect book for this audience. The book takes the huge amount of information available on network security and distills it into concise recommendations and instructions, using real world, step-by-step instruction. The latest addition to the best selling "How to Cheat..." series of IT handbooks, this book clearly identifies the primary vulnerabilities of most computer networks, including user access, remote access, messaging, wireless hacking, media, email threats, storage devices, and web applications. Solutions are provided for each type of threat, with emphasis on intrusion detection, prevention, and disaster recovery. * A concise information source - perfect for busy System Administrators with little spare time * Details what to do when disaster strikes your network * Covers the most likely threats to small to medium sized networks

When used with the MDX query language, SQL Server Analysis Services allows developers to build full-scale database applications to support such business functions as budgeting, forecasting, and market analysis. Shows readers how to build data warehouses and multi-dimensional databases, query databases, and use Analysis Services and other components of SQL Server to provide end-to-end solutions Revised, updated, and enhanced, the book discusses new features such as improved integration with Office and Excel 2007; query performance enhancements; improvements to aggregation designer, dimension designer, cube and dimension wizards, and cell writeback; extensibility and personalization; data mining; and more

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis. This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers. Comprehensive coverage of log management including analysis, visualization, reporting and more Includes information on different uses for logs -- from system operations to regulatory compliance Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

This book is about software piracy--what it is and how it's done. Stealing software is not to be condoned, and theft of intellectual property and copyright infringement are serious matters, but it's totally unrealistic to pretend that it doesn't happen. Software piracy has reached epidemic proportions. Many computer users know this, the software companies know this, and once you've read the Introduction to this book, you'll understand why. Seeing how widespread software piracy is, learning how it's accomplished, and particularly how incredibly easy it is to do might surprise you. This book describes how software piracy is actually being carried out. This book is about software piracy--what it is and how it's

done This is the first book ever to describe how software is actually stolen and traded over the internet Discusses security implications resulting from over 1/2 of the internet's computers running illegal, unpatched, pirated software

Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code. The book gives deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter. This book is intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code. * Winner of Best Book Bejtlich read in 2008! * <http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html> * Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader. * First book to detail how to perform "live forensic" techniques on malicious code. * In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Now in its third edition, Harlan Carvey has updated Windows Forensic Analysis Toolkit to cover Windows 7 systems. The primary focus of this edition is on analyzing Windows 7 systems and on processes using free and open-source tools. The book covers live response, file analysis, malware detection, timeline, and much more. The author presents real-life experiences from the trenches, making the material realistic and showing the why behind the how. New to this edition, the companion and toolkit materials are now hosted online. This material consists of electronic printable checklists, cheat sheets, free custom tools, and walk-through demos. This edition complements Windows Forensic Analysis Toolkit, 2nd Ed. (ISBN: 9781597494229), which focuses primarily on XP. Complete coverage and examples on Windows 7 systems Contains Lessons from the Field, Case Studies, and War Stories Companion online material, including electronic printable checklists, cheat sheets, free custom tools, and walk-through demos

Over 95% of computers around the world are running at least one Microsoft product. Microsoft Windows Software Update Service is designed to provide patches and updates to every one of these computers. The book will begin by describing the feature set of WSUS, and the benefits it provides to system administrators. Next, the reader will learn the steps that must be taken to configure their servers and workstations to make the compatible with WSUS. A special section then follows to help readers migrate from Microsoft's earlier update service, Software Update Service (SUS) to WSUS. The next chapters will then address the particular needs and complexities of managing WSUS on an enterprise network. Although WSUS is designed to streamline the update process, this service can still be a challenge for administrators to use effectively. To address these issues, the next chapters deal specifically with common problems that occur and the reader is provided with invaluable troubleshooting information. One of the other primary objectives of WSUS is to improve the overall security of Windows networks by ensuring that all systems have the most recent security updates and patches. To help achieve this goal, the next sections cover securing WSUS itself, so that critical security patches are always applied and cannot be compromised by malicious hackers. * Only book available on Microsoft's brand new, Windows Server Update Services * Employs Syngress' proven "How to Cheat" methodology providing readers with everything they need and nothing they don't * WSUS works with every Microsoft product, meaning any system administrator running a Windows-based network is a potential customer for this book

This book provides a comprehensive overview of the current and emerging challenges of cyber criminology, victimization and profiling. It is a compilation of the outcomes of the collaboration between researchers and practitioners in the cyber criminology field, IT law and security field. As Governments, corporations, security firms, and individuals look to tomorrow's cyber security challenges, this book provides a reference point for experts and forward-thinking analysts at a time when the debate over how we plan for the cyber-security of the future has become a major concern. Many criminological perspectives define crime in terms of social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition has allowed crime to be characterised, and crime prevention, mapping and measurement methods to be tailored to specific target audiences. However, this characterisation cannot be carried over to cybercrime, because the environment in which such crime is committed cannot be pinpointed to a geographical location, or distinctive social or cultural groups. Due to the rapid changes in technology, cyber criminals' behaviour has become dynamic, making it necessary to reclassify the typology being currently used. Essentially, cyber criminals' behaviour is evolving over time as they learn from their actions and others' experiences, and enhance their skills. The offender signature, which is a repetitive ritualistic behaviour that offenders often display at the crime scene, provides law enforcement agencies an appropriate profiling tool and offers investigators the opportunity to understand the motivations that perpetrate such crimes. This has helped researchers classify the type of perpetrator being sought. This book offers readers insights into the psychology of cyber criminals, and understanding and analysing

their motives and the methodologies they adopt. With an understanding of these motives, researchers, governments and practitioners can take effective measures to tackle cybercrime and reduce victimization.

Written by Microsoft's Log Parser developer, this is the first book available on Microsoft's popular yet undocumented log parser tool. The book and accompanying Web site contain hundreds of customized, working scripts and templates that system administrators will find invaluable for analyzing the log files from Windows Server, Snort IDS, ISA Server, IIS Server, Exchange Server, and other products. System administrators running Windows, Unix, and Linux networks manage anywhere from 1 to thousands of operating systems (Windows, Unix, etc.), Applications (Exchange, Snort, IIS, etc.), and hardware devices (firewalls, routers, etc.) that generate incredibly long and detailed log files of all activity on the particular application or device. This book will teach administrators how to use Microsoft's Log Parser to data mine all of the information available within these countless logs. The book teaches readers how all queries within Log Parser work (for example: a Log Parser query to an Exchange log may provide information on the origin of spam, viruses, etc.). Also, Log Parser is completely scriptable and customizable so the book will provide the reader with hundreds of original, working scripts that will automate these tasks and provide formatted charts and reports detailing the results of the queries. Written by Microsoft's sole developer of Log Parser, this is the first book available on the powerful yet completely undocumented product that ships with Microsoft's IIS, Windows Advanced Server 2003, and is available as a free download from the Microsoft Web site This book and accompanying scripts will save system administrators countless hours by scripting and automating the most common to the most complex log analysis tasks

This is the official CHFI (Computer Hacking Forensics Investigator) study guide for professionals studying for the forensics exams and for professionals needing the skills to identify an intruder's footprints and properly gather the necessary evidence to prosecute. The EC-Council offers certification for ethical hacking and computer forensics. Their ethical hacker exam has become very popular as an industry gauge and we expect the forensics exam to follow suit. Material is presented in a logical learning sequence: a section builds upon previous sections and a chapter on previous chapters. All concepts, simple and complex, are defined and explained when they appear for the first time. This book includes: Exam objectives covered in a chapter are clearly explained in the beginning of the chapter, Notes and Alerts highlight crucial points, Exam's Eye View emphasizes the important points from the exam's perspective, Key Terms present definitions of key terms used in the chapter, Review Questions contains the questions modeled after real exam questions based on the material covered in the chapter. Answers to the questions are presented with explanations. Also included is a full practice exam modeled after the real exam. The only study guide for CHFI, provides 100% coverage of all exam objectives. CHFI Training runs hundreds of dollars for self tests to thousands of dollars for classroom training.

The book begins with real world cases of botnet attacks to underscore the need for action. Next the book will explain botnet fundamentals using real world examples. These chapters will cover what they are, how they operate, and the environment and technology that makes them possible. The following chapters will analyze botnets for opportunities to detect, track, and remove them. Then the book will describe intelligence gathering efforts and results obtained to date. Public domain tools like OurMon, developed by Jim Binkley of Portland State University, will be described in detail along with discussions of other tools and resources that are useful in the fight against Botnets. This is the first book to explain the newest internet threat - Botnets, zombie armies, bot herders, what is being done, and what you can do to protect your enterprise Botnets are the most complicated and difficult threat the hacker world has unleashed - read how to protect yourself Over 700,000 IT Professionals Have Prepared for Exams with Syngress Authored Study Guides The Security+ Study Guide & Practice Exam is a one-of-a-kind integration of text and Web-based exam simulation and remediation. This system gives you 100% coverage of official CompTIA Security+ exam objectives plus test preparation software for the edge you need to achieve certification on your first try! This system is comprehensive, affordable, and effective! * Completely Guaranteed Coverage of All Exam Objectives All five Security+ domains are covered in full: General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography, and Operational / Organizational Security * Fully Integrated Learning This package includes a Study Guide and one complete practice exam. * Each chapter starts by explaining the exam objectives covered in the chapter You will always know what is expected of you within each of the exam's domains. * Exam-Specific Chapter Elements Notes, Tips, Alerts, Exercises, Exam's Eyeview, and Self Test with fully explained answers. * Test What You Learned Hundreds of self-test review questions test your knowledge of specific exam objectives. A Self Test Appendix features answers to all questions with complete explanations of correct and incorrect answers. Revision to market-leading first edition Realistic, Web-based practice exams included

With the proliferation of devices connected to the internet and connected to each other, the volume of data collected, stored, and processed is increasing every day, which brings new challenges in terms of information security. As big data expands with the help of public clouds, traditional security solutions tailored to private computing infrastructures and confined to a well-defined security perimeter, such as firewalls and demilitarized zones (DMZs), are no longer effective. New security functions are required to work over the heterogenous composition of diverse hardware, operating systems, and network domains. Security, Privacy, and Forensics Issues in Big Data is an essential research book that examines recent advancements in big data and the impact that these advancements have on information security and privacy measures needed for these networks. Highlighting a range of topics including cryptography, data analytics, and threat detection, this is an excellent reference source for students, software developers and engineers, security analysts, IT consultants, academicians, researchers, and professionals.

Windows Forensic Analysis DVD Toolkit, 2nd Edition, is a completely updated and expanded version of Harlan Carvey's best-selling forensics book on incident response and investigating cybercrime on Windows systems. With this book, you will learn how to analyze data during live and post-mortem investigations. New to this edition is Forensic Analysis on a Budget, which collects freely available tools that are essential for small labs, state (or below) law enforcement, and educational organizations. The book also includes new pedagogical elements, Lessons from the Field, Case Studies, and War Stories that present real-life experiences by an expert in the trenches, making the material real and showing the why behind the how. The companion DVD contains significant, and unique, materials (movies, spreadsheet, code, etc.) not available anyplace else because they were created by the author. This book will appeal to digital forensic investigators, IT security professionals, engineers, and system administrators as well as students and consultants. Best-Selling Windows Digital Forensic book completely updated in this 2nd Edition Learn how to Analyze Data During Live and Post-Mortem Investigations DVD Includes Custom Tools, Updated Code, Movies, and Spreadsheets!

The Network+ Study Guide covers all the objectives on the CompTIA exam, including the features and functions of networking components, and ensuring that readers have the knowledge and skills needed to install, configure and troubleshoot basic networking hardware, protocols and services. It covers exam topics such as media and topologies, protocols and standards, network implementation, and network support, as well as new exam topics on technologies such as wireless networking and Ethernet. * Complete coverage of the new 2005 exam, written from the ground up * Competitively priced with additional interactive exams online * Popular exam being revised for first time since 2001 Microsoft Log Parser Toolkit A Complete Toolkit for Microsoft's Undocumented Log Analysis Tool Elsevier

I decided to write this book for a couple of reasons. One was that I've now written a couple of books that have to do with incident response and forensic analysis on Windows systems, and I used a lot of Perl in both books. Okay...I'll come clean...I used nothing but Perl in both books! What I've seen as a result of this is that many readers want to use the

tools, but don't know how...they simply aren't familiar with Perl, with interpreted (or scripting) languages in general, and may not be entirely comfortable with running tools at the command line. This book is intended for anyone who has an interest in useful Perl scripting, in particular on the Windows platform, for the purpose of incident response, and forensic analysis, and application monitoring. While a thorough grounding in scripting languages (or in Perl specifically) is not required, it is helpful in fully and more completely understanding the material and code presented in this book. This book contains information that is useful to consultants who perform incident response and computer forensics, specifically as those activities pertain to MS Windows systems (Windows 2000, XP, 2003, and some Vista). My hope is that not only will consultants (such as myself) find this material valuable, but so will system administrators, law enforcement officers, and students in undergraduate and graduate programs focusing on computer forensics. *Perl Scripting for Live Response Using Perl, there's a great deal of information you can retrieve from systems, locally or remotely, as part of troubleshooting or investigating an issue. Perl scripts can be run from a central management point, reaching out to remote systems in order to collect information, or they can be "compiled" into standalone executables using PAR, PerlApp, or Perl2Exe so that they can be run on systems that do not have ActiveState's Perl distribution (or any other Perl distribution) installed. *Perl Scripting for Computer Forensic Analysis Perl is an extremely useful and powerful tool for performing computer forensic analysis. While there are applications available that let an examiner access acquired images and perform some modicum of visualization, there are relatively few tools that meet the specific needs of a specific examiner working on a specific case. This is where the use of Perl really shines through and becomes apparent. *Perl Scripting for Application Monitoring Working with enterprise-level Windows applications requires a great deal of analysis and constant monitoring. Automating the monitoring portion of this effort can save a great deal of time, reduce system downtimes, and improve the reliability of your overall application. By utilizing Perl scripts and integrating them with the application technology, you can easily build a simple monitoring framework that can alert you to current or future application issues.

Network Security Evaluation provides a methodology for conducting technical security evaluations of all the critical components of a target network. The book describes how the methodology evolved and how to define the proper scope of an evaluation, including the consideration of legal issues that may arise during the evaluation. More detailed information is given in later chapters about the core technical processes that need to occur to ensure a comprehensive understanding of the network's security posture. Ten baseline areas for evaluation are covered in detail. The tools and examples detailed within this book include both Freeware and Commercial tools that provide a detailed analysis of security vulnerabilities on the target network. The book ends with guidance on the creation of customer roadmaps to better security and recommendations on the format and delivery of the final report. * There is no other book currently on the market that covers the National Security Agency's recommended methodology for conducting technical security evaluations * The authors are well known in the industry for their work in developing and deploying network security evaluations using the NSA IEM * The authors also developed the NSA's training class on this methodology

Cisco IOS (the software that runs the vast majority of Cisco routers and all Cisco network switches) is the dominant routing platform on the Internet and corporate networks. This widespread distribution, as well as its architectural deficiencies, makes it a valuable target for hackers looking to attack a corporate or private network infrastructure. Compromised devices can disrupt stability, introduce malicious modification, and endanger all communication on the network. For security of the network and investigation of attacks, in-depth analysis and diagnostics are critical, but no book currently covers forensic analysis of Cisco network devices in any detail. Cisco Router and Switch Forensics is the first book devoted to criminal attacks, incident response, data collection, and legal testimony on the market leader in network devices, including routers, switches, and wireless access points. Why is this focus on network devices necessary? Because criminals are targeting networks, and network devices require a fundamentally different approach than the process taken with traditional forensics. By hacking a router, an attacker can bypass a network's firewalls, issue a denial of service (DoS) attack to disable the network, monitor and record all outgoing and incoming traffic, or redirect that communication anywhere they like. But capturing this criminal activity cannot be accomplished with the tools and techniques of traditional forensics. While forensic analysis of computers or other traditional media typically involves immediate shut-down of the target machine, creation of a duplicate, and analysis of static data, this process rarely recovers live system data. So, when an investigation focuses on live network activity, this traditional approach obviously fails. Investigators must recover data as it is transferred via the router or switch, because it is destroyed when the network device is powered down. In this case, following the traditional approach outlined in books on general computer forensics techniques is not only insufficient, but also essentially harmful to an investigation. Jargon buster: A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). A router is a more sophisticated network device that joins multiple wired or wireless networks together. The only book devoted to forensic analysis of routers and switches, focusing on the operating system that runs the vast majority of network devices in the enterprise and on the Internet Outlines the fundamental differences between router forensics and traditional forensics, a critical distinction for responders in an investigation targeting network activity Details where network forensics fits within the entire process of an investigation, end to end, from incident response and data collection to preparing a report and legal testimony

Umer Khan's first book, Cisco Security Specialist's Guide to PIX Firewalls, ISBN: 1931836639, has consistently maintained its spot as the #1 best-selling PIX book on amazon.com by providing readers with a clear, comprehensive, and independent introduction to PIX Firewall configuration. With the market for PIX Firewalls maintaining double digit growth and several major enhancements to both the PIX Firewall and VPN Client product lines, this book will have enormous appeal with the audience already familiar with his first book. The Cisco Pix firewall is the #1 market leading

firewall, owning 43% market share. Cisco is poised to release the newest, completely re-designed version 7 of the Pix operating system in the first quarter of 2004 "Cisco Pix Firewalls: configure | manage | troubleshoot" Covers all objectives on the new Cisco Pix certification exam, making this book the perfect study guide in addition to professional reference Umer Khan's first book "Cisco Security Specialist's Guide to PIX Firewall" has been the #1 market leading Cisco Pix book since it was published in 2002

Well respected, practical reference guide to Microsoft Windows Server 2003 that now covers the "R2" update.

CD and DVD Forensics will take the reader through all facets of handling, examining, and processing CD and DVD evidence for computer forensics. At a time where data forensics is becoming a major part of law enforcement and prosecution in the public sector, and corporate and system security in the private sector, the interest in this subject has just begun to blossom. CD and DVD Forensics is a how to book that will give the reader tools to be able to open CDs and DVDs in an effort to identify evidence of a crime. These tools can be applied in both the public and private sectors.

Armed with this information, law enforcement, corporate security, and private investigators will be able to be more effective in their evidence related tasks. To accomplish this the book is divided into four basic parts: (a) CD and DVD physics dealing with the history, construction and technology of CD and DVD media, (b) file systems present on CDs and DVDs and how these are different from that which is found on hard disks, floppy disks and other media, (c)

considerations for handling CD and DVD evidence to both recover the maximum amount of information present on a disc and to do so without destroying or altering the disc in any way, and (d) using the InfinaDyne product CD/DVD Inspector to examine discs in detail and collect evidence. This is the first book addressing using the CD/DVD Inspector product in a hands-on manner with a complete step-by-step guide for examining evidence discs See how to open CD's and DVD's and extract all the crucial evidence they may contain

A One-Stop Reference Containing the Most Read Topics in the Syngress Security Library This Syngress Anthology Helps You Protect Your Enterprise from Tomorrow's Threats Today This is the perfect reference for any IT professional responsible for protecting their enterprise from the next generation of IT security threats. This anthology represents the "best of this year's top Syngress Security books on the Human, Malware, VoIP, Device Driver, RFID, Phishing, and Spam threats likely to be unleashed in the near future.. * From Practical VoIP Security, Thomas Porter, Ph.D. and Director of IT Security for the FIFA 2006 World Cup, writes on threats to VoIP communications systems and makes recommendations on VoIP security. * From Phishing Exposed, Lance James, Chief Technology Officer of Secure Science Corporation, presents the latest information on phishing and spam. * From Combating Spyware in the Enterprise, Brian Baskin, instructor for the annual Department of Defense Cyber Crime Conference, writes on forensic detection and removal of spyware. * Also from Combating Spyware in the Enterprise, About.com's security expert Tony Bradley covers the transformation of spyware. * From Inside the SPAM Cartel, Spammer-X shows how spam is created and why it works so well. * From Securing IM and P2P Applications for the Enterprise, Paul Piccard, former manager of Internet Security Systems' Global Threat Operations Center, covers Skype security. * Also from Securing IM and P2P Applications for the Enterprise, Craig Edwards, creator of the IRC security software IRC Defender, discusses global IRC security. * From RFID Security, Brad "Renderman Haines, one of the most visible members of the wardriving community, covers tag encoding and tag application attacks. * Also from RFID Security, Frank Thornton, owner of Blackthorn Systems and an expert in wireless networks, discusses management of RFID security. * From Hack the Stack, security expert Michael Gregg covers attacking the people layer. * Bonus coverage includes exclusive material on device driver attacks by Dave Maynor, Senior Researcher at SecureWorks. * The "best of this year: Human, Malware, VoIP, Device Driver, RFID, Phishing, and Spam threats * Complete Coverage of forensic detection and removal of spyware, the transformation of spyware, global IRC security, and more * Covers secure enterprise-wide deployment of hottest technologies including Voice Over IP, Pocket PCs, smart phones, and more

[Copyright: 7a080e4a8d4c3922c995476f6c06363b](#)