

Understanding Wmi Scripting Exploiting Microsofts Windows Management Instrumentation In Mission Critical Computing Infrastructures Hp Technologies

Like Sun Tzu's Art of War for Modern Business, this book uses ancient ninja scrolls as the foundation for teaching readers about cyber-warfare, espionage and security. Cyberjutsu is a practical cybersecurity field guide based on the techniques, tactics, and procedures of the ancient ninja. Cyber warfare specialist Ben McCarty's analysis of declassified Japanese scrolls will show how you can apply ninja methods to combat today's security challenges like information warfare, deceptive infiltration, espionage, and zero-day attacks. Learn how to use key ninja techniques to find gaps in a target's defense, strike where the enemy is negligent, master the art of invisibility, and more. McCarty outlines specific, in-depth security mitigations such as fending off social engineering attacks by being present with "the correct mind," mapping your network like an adversary to prevent breaches, and leveraging ninja-like traps to protect your systems. You'll also learn how to:

- Use threat modeling to reveal network vulnerabilities
- Identify insider threats in your organization
- Deploy countermeasures like network sensors, time-based controls, air gaps, and authentication protocols
- Guard against malware command and-control servers
- Detect attackers, prevent supply-chain attacks, and counter zero-day exploits

Cyberjutsu is the playbook that every modern cybersecurity professional needs to channel their inner ninja. Turn to the old ways to combat the latest cyber threats and stay one step ahead of your adversaries.

Pour assurer les tâches de planification, de configuration et d'administration au sein d'une infrastructure Active Directory et aussi pour surveiller et maintenir la disponibilité et les performances de ces services d'annuaire : DNS, opérations LDAP, certificats X.509v3, PKI, structure physique, groupes, OUs et délégation, services d'infrastructure, stratégies de groupe, maintenance...

Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker's Handbook, Fifth Edition explains the enemy's current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition.

- Build and launch spoofing exploits with Ettercap
- Induce error conditions and crash software using fuzzers
- Use advanced reverse engineering to exploit Windows and Linux software
- Bypass Windows Access Control and memory protection schemes
- Exploit web applications with Padding Oracle Attacks
- Learn the use-after-free technique used in recent zero days
- Hijack web browsers with advanced XSS attacks
- Understand ransomware and how it takes control of your desktop
- Dissect Android malware with JEB and DAD decompilers
- Find one-day vulnerabilities with binary diffing
- Exploit wireless systems with Software Defined Radios (SDR)
- Exploit Internet of things devices
- Dissect and exploit embedded devices
- Understand bug bounty programs
- Deploy next-generation honeypots
- Dissect ATM malware and analyze common ATM attacks
- Learn the business side of ethical hacking

Covers the installation and components of WMI, its interactions and subsystems, query language facilities, class schemas, method design, and developing management and .NET management applications.

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

Special Ops: Internal Network Security Guide is the solution for the impossible 24-hour IT work day. By now, most companies have hardened their perimeters and locked out the "bad guys," but what has been done on the inside? This book attacks the problem of the soft, chewy center in internal networks. We use a two-pronged approach-Tactical and Strategic-to give readers a complete guide to internal penetration testing. Content includes the newest vulnerabilities and exploits, assessment methodologies, host review guides, secure baselines and case studies to bring it all together. We have scoured the Internet and assembled some of the best to function as Technical Specialists and Strategic Specialists. This creates a diversified project removing restrictive corporate boundaries. The unique style of this book will allow it to cover an incredibly broad range of topics in unparalleled detail. Chapters within the book will be written using the same concepts behind software development. Chapters will be treated like functions within programming code, allowing the authors to call on each other's data. These functions will supplement the methodology when specific technologies are examined thus reducing the common redundancies found in other security books. This book is designed to be the "one-stop shop" for security engineers who want all their information in one place. The technical nature of this may be too much for middle management; however technical managers can use the book to help them understand the challenges faced by the engineers who support their businesses. Ø Unprecedented Team of Security Luminaries. Led by Foundstone Principal Consultant, Erik Pace Birkholz, each of the contributing authors on this book is a recognized superstar in their respective fields. All are highly visible speakers and consultants and their frequent presentations at major industry events such as the Black Hat Briefings and the 29th Annual Computer Security Institute Show in November, 2002 will provide this book with a high-profile launch. Ø The only all-encompassing book on internal network security. Windows 2000, Windows XP, Solaris, Linux and Cisco IOS and their applications are usually running simultaneously in some form on most enterprise networks. Other books deal with these components individually, but no other book provides a comprehensive solution like Special Ops. This book's unique style will give the reader the value of 10 books in 1.

The definitive guide to scripting for all Windows administrators helps them to simplify their work and make their network more secure. Jones demystifies scripting, showing how VBScript and WMI can help ease repetitive or complex tasks. Based on the author's years of experience teaching and training, the book covers Windows NT, Windows 2000, Windows XP, and Windows 2003.

Provides instructions for automating Windows 2000 administrative tasks using scripting techniques in order to complete routine tasks in core administration areas.

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including:

Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekal 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

An in-depth look at the radical changes to the newest release of SSISS Microsoft SQL Server 2012 Integration Services (SISS) builds on the revolutionary database product suite first introduced in 2005. With this crucial resource, you will explore how this newest release serves as a powerful tool for performing extraction, transformation, and load operations (ETL). A team of SQL Server experts deciphers this complex topic and provides detailed coverage of the new features of the 2012 product release. In addition to technical updates and additions, the authors present you with a new set of SISS best practices, based on years of real-world experience that have transpired since the previous edition was published.

Details the newest features of the 2012 SISS product release, which is the most significant release since 2005

Addresses the keys to a successful ETL solution, such as using the right enterprise ETL tool and employing the right ETL architecture in order to meet the system requirements Includes additional case studies and tutorial examples to illustrate advanced concepts and techniques Professional Microsoft SQL Server 2012 Integration Services is a valuable resource that meets the demands and high expectations of experienced SSIS professionals.

Annotation Learn to design and implement sophisticated management solutions in Windows 2000 using WMI. All the WMI topics and examples are illustrated with fully functional real-world script examples that can be used as is on the reader's network. Lavy and Meggitt are widely recognized as WMI gurus. The material takes readers from a fundamental understanding of WMI and empowers them with the ability to design and implement their own sophisticated management solutions. Windows Management Instrumentation (WMI) is a new technology from Microsoft that has the potential to transform the administration of windows-based networks. System administrators will seek detailed, hands-on advice on using this revolutionary tool. This book tells readers everything they need to know in order to harness the power of WMI to automate vast parts of Windows 2000 workstation and server management. Starting with the absolute basics, teaching the fundamentals of WMI terminology and the VBScript programming language. By the time readers complete the book, the readers will have the ability not only to use the scripts supplied, but also have a good understanding both of WMI and VBScript. Scripts from the book and tools referenced by the authors will be available at: www.newriders.com Matthew Lavy, MA, MPhil, ARCM, LTCL, is Technical Systems Developer at Jesus College, Cambridge University. His main responsibilities are developing solutions for UNIX / NT systems integration and providing technical support to Windows 2000 systems administrators. He has been both an author and technical reviewer for the O'reilly Windows NT series, and is a member of the Cambridge University Windows 2000 technical strategy group. Ashley Meggitt, MSc, is IT Manager for Jesus College, Cambridge University, responsible for the management of the IT Department and for formulating the College's long-term IT strategy. He is the co-author of two books on Windows NT system administration, both published by O'reilly, for whom he has also acted as a technical reviewer.

The popular open source KDE desktop environment for Unix was built with Qt, a C++ class library for writing GUI applications that run on Unix, Linux, Windows 95/98, Windows 2000, and Windows NT platforms. Qt emulates the look and feel of Motif, but is much easier to use. Best of all, after you have written an application with Qt, all you have to do is recompile it to have a version that works on Windows. Qt also emulates the look and feel of Windows, so your users get native-looking interfaces. Platform independence is not the only benefit. Qt is flexible and highly optimized. You'll find that you need to write very little, if any, platform-dependent code because Qt already has what you need. And Qt is free for open source and Linux development. Although programming with Qt is straightforward and feels natural once you get the hang of it, the learning curve can be steep. Qt comes with excellent reference documentation, but beginners often find the included tutorial is not enough to really get started with Qt. That's where Programming with Qt steps in. You'll learn how to program in Qt as the book guides you through the steps of writing a simple paint application. Exercises with fully worked out answers help you deepen your understanding of the topics. The book presents all of the GUI elements in Qt, along with advice about when and how to use them, so you can make full use of the toolkit. For seasoned Qt programmers, there's also lots of information on advanced 2D transformations, drag-and-drop, writing custom image file filters, networking with the new Qt Network Extension, XML processing, Unicode handling, and more. Programming with Qt helps you get the most out of this powerful, easy-to-use, cross-platform toolkit. It's been completely updated for Qt Version 3.0 and includes entirely new information on rich text, Unicode/double byte characters, internationalization, and network programming.

The latest Windows security attack and defense strategies "Securing Windows begins with reading this book." --James Costello (CISSP) IT Security Specialist, Honeywell Meet the challenges of Windows security with the exclusive Hacking Exposed "attack-countermeasure" approach. Learn how real-world malicious hackers conduct reconnaissance of targets and then exploit common misconfigurations and software flaws on both clients and servers. See leading-edge exploitation techniques demonstrated, and learn how the latest countermeasures in Windows XP, Vista, and Server 2003/2008 can mitigate these attacks. Get practical advice based on the authors' and contributors' many years as security professionals hired to break into the world's largest IT infrastructures. Dramatically improve the security of Microsoft technology deployments of all sizes when you learn to: Establish business relevance and context for security by highlighting real-world risks Take a tour of the Windows security architecture from the hacker's perspective, exposing old

and new vulnerabilities that can easily be avoided Understand how hackers use reconnaissance techniques such as footprinting, scanning, banner grabbing, DNS queries, and Google searches to locate vulnerable Windows systems Learn how information is extracted anonymously from Windows using simple NetBIOS, SMB, MSRPC, SNMP, and Active Directory enumeration techniques Prevent the latest remote network exploits such as password grinding via WMI and Terminal Server, passive Kerberos logon sniffing, rogue server/man-in-the-middle attacks, and cracking vulnerable services See up close how professional hackers reverse engineer and develop new Windows exploits Identify and eliminate rootkits, malware, and stealth software Fortify SQL Server against external and insider attacks Harden your clients and users against the latest e-mail phishing, spyware, adware, and Internet Explorer threats Deploy and configure the latest Windows security countermeasures, including BitLocker, Integrity Levels, User Account Control, the updated Windows Firewall, Group Policy, Vista Service Refactoring/Hardening, SafeSEH, GS, DEP, Patchguard, and Address Space Layout Randomization

Go beyond simple queries and get the inside track on how to write system administration scripts with Windows Management Instrumentation (WMI)—straight from a Microsoft scripting expert. With labs and lessons you complete at your own pace, this definitive tutorial helps you build your scripting expertise and provides the professional guidance you need to automate Windows administrative tasks. Teach yourself how to write and run scripts to: Configure WMI—without editing the registry Audit and inventory software on local or remote desktops and servers Manage system components, including keyboards, motherboards, disk drives, and printers Monitor and report on real-time changes in system performance and respond to critical events Configure network components Test security access rights and make changes to one or multiple systems And learn how to: Test, diagnose, and resolve errors with WMI Back-up and restore the registry PLUS—Get more than 900 script samples that you can use to help simplify the management of your system resources CD-ROM features: More than 900 sample scripts to adapt for your own work Time-saving scripting tools—including Script-o-Matic 2.0 and WMIcheck Fully searchable eBook A Note Regarding the CD or DVD The print version of this book ships with a CD or DVD. For those customers purchasing one of the digital formats in which this book is available, we are pleased to offer the CD/DVD content as a free download via O'Reilly Media's Digital Distribution services. To download this content, please visit O'Reilly's web site, search for the title of this book to find its catalog page, and click on the link below the cover image (Examples, Companion Content, or Practice Files). Note that while we provide as much of the media content as we are able via free download, we are sometimes limited by licensing restrictions. Please direct any questions or concerns to booktech@oreilly.com.

Summary PowerShell and WMI is an example-driven guide for administrators managing networks of Windows servers and desktops. With 150 practical examples, including ready-to-reuse scripts and techniques, you'll learn the ins and outs of automating WMI via PowerShell v3. You'll also find deep coverage of all aspects of Windows administration, including IIS, DNS and Hyper-V. About the Technology WMI, on its own, is simply a collection of Windows management facilities. Paired with PowerShell, however, WMI becomes a brilliant toolset for automating servers, networks, and remote Windows computers. About the Book PowerShell and WMI is an industrial-strength guide for administrators of Windows networks, servers, and desktops. You'll start with practical overviews of PowerShell and of WMI. Then you'll explore 150 specific examples—all with ready-to-use scripts—designed to simplify your day-to-day system management. Each tested technique is configured to load as part of a PowerShell module. A set of handy appendixes includes references for PowerShell and WMI. Prior exposure to PowerShell and WMI is helpful but not required. Purchase of the print book comes with an offer of a free PDF, ePub, and Kindle eBook from Manning. Also available is all code from the book. What's Inside Managing Windows, IIS, and Hyper-V Remote desktops and devices Logs, jobs, and performance New PowerShell v3 WMI functionality ===== Table of Contents PART 1 TOOLS OF THE TRADE Solving administrative challenges Using PowerShell WMI in depth Best practices and optimization PART 2 WMI IN THE ENTERPRISE? System documentation Disk systems Registry administration Filesystem administration Services and processes Printers Configuring network adapters Managing IIS Configuring a server Users and security Logs, jobs, and performance Administering Hyper-V with PowerShell and WMI PART 3 THE FUTURE: POWERSHELL V3 AND WMI WMI over WSMAN Your own WMI cmdlets CIM cmdlets and sessions

Understanding WMI Scripting explains to Windows and Exchange Administrators how they can use the Windows Management Instrumentation (WMI) scriptable technology available in these products to ease their day-to-day management tasks. Under Windows.NET and Exchange 2000 (SP2), Microsoft is making solid enhancements in WMI. This will dramatically extend the scripting and manageability capabilities of Windows and Exchange. Illustrated with more than three hundred samples, the book links practical problems encountered by administrators to applicable scriptable solutions. Lissour focuses not on MI programming aspects for developers but on how administrators can use what is available in Windows and Exchange for their admin work. WMI is a very important topic under Windows.NET and Exchange 2000 (SP2), so this book provides real added value to Windows/Exchange administrators. Although Exchange relies on Windows, no other book combines coverage of Windows and Exchange. · Fine tune management of Windows servers · Achieve better system management and customize critical operations · Access hundreds of usable scripts in book and downloadable from web

A guide to VBScript covers such topics as building scripting components, Active Directory, using Windows Management Instrumentation techniques, building hypertext applications, and creating security-enhanced scripts.

Provides techniques and methods to design, deploy and manage an Exchange Server operation. Describes exchange "best practices" developed by author and his colleagues at Compaq.

Prepare for Microsoft Exam MS-101—and help demonstrate your real-world mastery of skills and knowledge needed to manage Microsoft 365 mobility, security, and related administration tasks. Designed for experienced IT professionals, Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified Expert level. Focus on the expertise measured by these objectives:

Implement modern device services Implement Microsoft 365 security and threat management Manage Microsoft 365 governance and compliance This Microsoft Exam Ref: Organizes its coverage by exam objectives Features strategic, what-if scenarios to challenge you Assumes you are a Microsoft 365 Enterprise Administrator who participates in evaluating, planning, migrating, deploying, and managing Microsoft 365 services About the Exam Exam MS-101 focuses on knowledge needed to implement Mobile Device Management (MDM); manage device compliance; plan for devices and apps; plan Windows 10 deployment; implement Cloud App Security (CAS), threat management, and Windows Defender Advanced Threat Protection (ATP); manage security reports and alerts; configure Data Loss Prevention (DLP); implement Azure Information Protection (AIP); and manage data governance, auditing, and eDiscovery. About Microsoft Certification Passing this exam and Exam MS-100 Microsoft 365 Identity and Services (and earning one Microsoft 365 workload administrator certification or the MCSE: Productivity certification) fulfills your requirements for the Microsoft 365 Certified: Enterprise Administrator Expert certification credential. This demonstrates your ability to evaluate, plan, migrate, deploy, and manage Microsoft 365 services. See full details at: microsoft.com/learn

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CompTIA Pentest+ PT0-001 exam success with this CompTIA Cert Guide from Pearson IT Certification, a leader in IT Certification. Master CompTIA Pentest+ PT0-001 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Practice with realistic exam questions Get practical guidance for next steps and more advanced certifications CompTIA Pentest+ Cert Guide is a best-of-breed exam study guide. Leading IT security experts Omar Santos and Ron Taylor share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The CompTIA study guide helps you master all the topics on the Pentest+ exam, including: Planning and scoping: Explain the importance of proper planning and scoping, understand key legal concepts, explore key aspects of compliance-based assessments Information gathering and vulnerability identification: Understand passive and active reconnaissance, conduct appropriate information gathering and use open source intelligence (OSINT); perform vulnerability scans; analyze results; explain how to leverage gathered information in exploitation; understand weaknesses of specialized systems Attacks and exploits: Compare and contrast social engineering attacks; exploit network-based, wireless, RF-based, application-based, and local host vulnerabilities; summarize physical security attacks; perform post-exploitation techniques Penetration testing tools: Use numerous tools to perform reconnaissance, exploit vulnerabilities and perform post-exploitation activities; leverage the Bash shell, Python, Ruby, and PowerShell for basic scripting Reporting and communication: Write reports containing effective findings and recommendations for mitigation; master best practices for reporting and communication; perform post-engagement activities such as cleanup of tools or shells

Manage and maintain your Microsoft Exchange 2010 environment with Windows PowerShell 2.0 and the Exchange Management Shell. Coding for Penetration Testers: Building Better Tools, Second Edition provides readers with an understanding of the scripting languages that are commonly used when developing tools for penetration testing, also guiding users through specific examples of custom tool development and the situations where such tools might be used. While developing a better understanding of each language, the book presents real-world scenarios and tool development that can be incorporated into a tester's toolkit. This completely updated edition focuses on an expanded discussion on the use of Powershell, and includes practical updates to all tools and coverage. Discusses the use of various scripting languages in penetration testing Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages Provides a primer on scripting, including, but not limited to, web scripting, scanner scripting, and exploitation scripting Includes all-new coverage of Powershell

Description des concepts et de l'administration du service DNS et de son intégration dans Active Directory. Point sur les composants de la structure logique (domaines, OU, arbres, forêts...) et sur la création et la configuration d'objets stratégies de groupe (GPMC, RSoP, délégation...).

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CCNA Cyber Ops SECFND 210-250 exam success with this Cert Guide from Pearson IT Certification, a leader in IT Certification learning. Master CCNA Cyber Ops SECFND 210-250 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks CCNA Cyber Ops SECFND 210-250 Official Cert Guide is a best-of-breed exam study guide. Cisco enterprise security experts Omar Santos, Joseph Muniz, and Stefano De Crescenzo share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The study guide helps you master all the topics on the CCNA Cyber Ops SECFND exam, including: Fundamentals of networking protocols and networking device types Network security devices and cloud services Security principles Access control models Security management concepts and techniques Fundamentals of cryptography and PKI Essentials of Virtual Private Networks (VPNs) Windows-based Analysis Linux /MAC OS X-based Analysis Endpoint security technologies Network and host telemetry Security monitoring operations and challenges Types of attacks and vulnerabilities Security evasion techniques Provides information on using Microsoft Virtual Server 2005, covering such topics as creating a virtual network, installing automated deployment services, creating a virtual machine using scripts, and migrating physical servers to a virtual environment.

Know how to set up, defend, and attack computer networks with this revised and expanded second edition. You will learn to configure your network from the ground up, beginning with developing your own private virtual test environment, then setting up your own DNS server and AD infrastructure. You will continue with more advanced network services, web servers, and database servers and you will end by building your own web applications servers, including WordPress and Joomla!. Systems from 2011 through 2017 are covered, including Windows 7, Windows 8, Windows 10, Windows Server 2012, and Windows Server 2016 as well as a range of Linux distributions, including Ubuntu, CentOS, Mint, and OpenSUSE. Key defensive techniques are integrated throughout and you will develop situational awareness of your network and build a complete defensive infrastructure, including log servers, network firewalls, web application firewalls, and intrusion detection systems. Of course, you cannot truly understand how to defend a network if you do not know how to attack it, so you will attack your test systems in a variety of ways. You will learn about Metasploit, browser attacks, privilege escalation, pass-the-hash attacks, malware, man-in-the-middle attacks, database attacks, and web application attacks. What You'll Learn Construct a testing laboratory to experiment with

software and attack techniques Build realistic networks that include active directory, file servers, databases, web servers, and web applications such as WordPress and Joomla! Manage networks remotely with tools, including PowerShell, WMI, and WinRM Use offensive tools such as Metasploit, Mimikatz, Veil, Burp Suite, and John the Ripper Exploit networks starting from malware and initial intrusion to privilege escalation through password cracking and persistence mechanisms Defend networks by developing operational awareness using auditd and Sysmon to analyze logs, and deploying defensive tools such as the Snort intrusion detection system, IPFire firewalls, and ModSecurity web application firewalls Who This Book Is For This study guide is intended for everyone involved in or interested in cybersecurity operations (e.g., cybersecurity professionals, IT professionals, business professionals, and students)

Transform Raw Data Into Meaningful Business Intelligence with SSIS Deploy and manage high-performance data transformation solutions across your enterprise using the step-by-step techniques in this fully revised guide. Hands-On Microsoft SQL Server 2008 Integration Services, Second Edition explains the tools and methods necessary to extract conclusive business intelligence from disparate corporate data. Learn how to build and secure packages, load and cleanse data, establish workflow, and optimize performance. Real-world examples, detailed illustrations, and hands-on exercises are included throughout this practical resource. Build SSIS packages using the Import and Export Wizard and Business Intelligence Development Studio Create Loop and Task Host Containers with Control Flow Designer Administer SSIS from SQL Server Management Studio and dutil Secure packages using encryption, roles, signatures, and permissions Build-in memory lookups and transformations using the Data Flow Engine Extend functionality using custom scripts and ActiveX components Use SCD transformations to load data warehouses and data marts Learn to build a Star Schema and Parallel Data Warehouse Migrate Data Transformation Services 2000 and SSIS 2005 packages

Provides information on Windows Vista security issues and tools, covering such topics as password management, e-mail security, firewalls, browser security, data protection, network security protecting against viruses and spyware, and using encryption.

With over 40% new and revised material throughout the book, this updated version provides thorough coverage of implementation, migration and management issues for Exchange 2000 and 2003, all backed up by best practices developed by HP, Microsoft's only world-wide Prime Integrator for Exchange. The best and most comprehensive coverage of Exchange from the Chief Technology Officer of HP Services, Microsoft's only worldwide Prime Integrator for Windows and Exchange. - With over 40% new and revised material throughout the book, this updated version provides thorough coverage of implementation, migration and management issues for Exchange 2000 and 2003, all backed up by best practices developed by HP, Microsoft's only world-wide Prime Integrator for Exchange. - New coverage of Exchange Intelligent Message Filter - Revised and updated coverage of best practices for the design, deployment, and operation of Exchange 2003 -

Comprehensive treatment of major issues facing email deployments, including anti-virus and anti-spam techniques - Review of Microsoft's future strategy for Exchange since dropping the Kodiak approach

Prepare for the CEH training course and exam by gaining a solid foundation of knowledge of key fundamentals such as operating systems, databases, networking, programming, cloud, and virtualization. Based on this foundation, the book moves ahead with simple concepts from the hacking world. The Certified Ethical Hacker (CEH) Foundation Guide also takes you through various career paths available upon completion of the CEH course and also prepares you to face job interviews when applying as an ethical hacker. The book explains the concepts with the help of practical real-world scenarios and examples. You'll also work with hands-on exercises at the end of each chapter to get a feel of the subject. Thus this book would be a valuable resource to any individual planning to prepare for the CEH certification course.

What You Will Learn Gain the basics of hacking (apps, wireless devices, and mobile platforms) Discover useful aspects of databases and operating systems from a hacking perspective Develop sharper programming and networking skills for the exam Explore the penetration testing life cycle Bypass security appliances like IDS, IPS, and honeypots Grasp the key concepts of cryptography Discover the career paths available after certification Revise key interview questions for a certified ethical hacker Who This Book Is For Beginners in the field of ethical hacking and information security, particularly those who are interested in the CEH course and certification.

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. In-depth coverage of Microsoft's powerful new data integration tool Learn to maximize the features of SQL Server 2005 Integration Services from this essential guide. Hands-On Microsoft SQL Server 2005 Integration Services makes learning SSIS easy through the use of extensive real-world exercises structured around every component within the tool. You will learn to collect corporate data from various sources and transform that data for analysis, mining, and reporting.

Microsoft SharePoint 2013 Unleashed is the newest version of the best-selling SharePoint Unleashed series by Michael Noel and Colin Spence. Once again, Noel and Spence deliver comprehensive, real-world coverage of everything you need to know to successfully design, implement, configure and use SharePoint 2013 solutions. Leveraging their experience with hundreds of companies of all sizes and from many different industries, Noel and Spence present best practices and expert implementation and configuration methodologies, and focus on the features and tools that provide the most value to busy professionals. This edition adds comprehensive coverage of SharePoint 2013's most valuable and productive new features, including: Using PowerShell automation to streamline management Building virtualized SharePoint environments Strengthening authentication and security Improving user experience via the ribbon interface; new lists, libraries, and templates; and enhanced metadata Integrating with the newest versions of Microsoft Office, Exchange, SQL Server, ForeFront, and System Center Taking full advantage of key mobile and social improvements Using the newest Business Connectivity Services capabilities Improving records management/compliance, web content management, and BI And much more Noel and Spence also offer indispensable guidance on migration, UI, and data store choices, and dependencies; and present crucial infrastructure knowledge that most SharePoint guides ignore.

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

Understanding WMI Scripting Exploiting Microsoft's Windows Management Instrumentation in Mission-Critical Computing Infrastructures Elsevier

An update to a classic reference published fifteen years ago, this publication concerns the theoretical aspects of inductive electromagnetic methods applied in geophysical prospecting. From first principles, the electromagnetic responses of several models are derived and analysed in order to form a strong basis for understanding such phenomenon in practice. The original

work has been extended by using modern 3-D modeling capabilities with a special emphasis on airborne applications. Exploration and research geophysicists will appreciate the numerous closed-form and asymptotic electromagnetic expressions for spherical and cylindrical conductors contained within non-conductive and conductive hosts which are described in this volume. Responses based on such expressions are often presented in graphical and tabular form in order to help the reader visualise the significance of the results and in order to facilitate comparisons with physical and numerical modeling results. In contrast to the first edition, key results are summarised at the end of each chapter and old material that has been retained in the new edition has been clarified and in many instances corrected. A new chapter has been written in which an extensive evaluation of several different airborne electromagnetic systems is described. The evaluation was based on the utilization of an advanced 3-D modeling program to simulate complex geoelectrical situations that are of interest in exploration and in airborne resistivity mapping.

Leveraging WMI Scripting is the second in a series of two books dedicated to WMI. Understanding WMI Scripting (ISBN 1-55558-266-4), Lissair's first book, explained to Windows Administrators the various WMI scripting techniques and manageability capabilities of this new Windows Server 2003 platform. Illustrated with hundreds of scripts and detailed tables, the book explained the underlying technology and how WMI can be put to work. Lissair focused not only on WMI programming aspects for developers but on how administrators can use what is available in Windows for their admin work. If you've had significant WMI experience, or have read Lissair's first book, you are ready to apply your WMI knowledge to any technology that interfaces with WMI. Leveraging WMI Scripting continues the presentation of WMI begun in Understanding WMI Scripting. In this new volume, we dive deeper into WMI to understand the manageable entities of the Windows world. Lissair offers a structured description of the most important WMI providers available from Windows NT 4.0 to Windows Server 2003 (including Windows 2000 and Windows XP). This covers the WMI management of the Windows Registry, Active Directory, SNMP, the Resultant Set Of Policies (RSOP), and the Volume Shadow Service to name a few. This discussion leverages the information on building real-world scripted management solutions presented in Lissair's first book. Like the first volume, Leveraging WMI Scripting is based on an important concept: "learning by practice." Leveraging WMI Scripting addresses the most advanced topics so that you can exploit the features of various WMI interfaces to manage the components in a real-world environment. WMI is a critical topic under Windows Server 2003, so this book provides real added value to every Windows administrator.

- Shows you how to extract data from applications, understand what's really happening on your servers, and get real work done
- Provides hundreds of usable scripts to use in everyday solutions for network performance and security
- Offers practical and straightforward advice that any enterprise Windows administrator can learn from

Your hands-on guide to Windows PowerShell scripting fundamentals Expand your expertise--and teach yourself the fundamentals of Windows PowerShell scripting, including features available in Windows PowerShell 5. If you are an IT professional, power user, or consultant, you'll get the guidance, exercises, and code you need to master core techniques for automating Windows setup, deployment, and management. Discover how to: Run cmdlets and command-line utilities Administer Windows-based servers and desktops with built-in cmdlets Use providers to access external information Write and run scripts from the Windows ISE Create functions that are easy to maintain Build standardized environments with profiles Automate Windows systems with WMI, CIM cmdlets, and remoting Automate Active Directory Domain Services (AD DS) Debug scripts and handle errors Run commands that survive interruptions Use Desired State Configuration (DSC) to manage software services and their environments Get powerful new modules from PowerShell Gallery About You This book is for: IT professionals and power users who want to get productive with Windows PowerShell, including new features in Windows PowerShell 5 Windows system administrators who want to be more efficient and productive Anyone pursuing Windows PowerShell certifications No experience with Windows PowerShell or other scripting technologies necessary

[Copyright: a5fd01b960d029983952e863185e0bd8](#)