# Network Security With Netflow And Ipfix Big Data Analytics For Information Security Networking Technology

Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey brings together a few top experts to create the first detailed guide for professionals who are already familiar with digital evidence. The Handbook of Computer Crime Investigation helps readers master the forensic analysis of computer systems with a three-part approach covering tools, technology, and case studies. The Tools section provides the details on leading software programs, with each chapter written by that product's creator. The section ends with an objective comparison of the strengths and limitations of each tool. The main Technology section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, moving on to networks, and culminating with embedded systems. The Case Examples section gives readers a sense of the technical, legal, and practical challenges that arise in real computer investigations. The Tools section provides details of leading hardware and software The main Technology section provides the technical "how to" information for collecting and analysing digital evidence in common situations Case Examples give readers a sense of the technical, legal, and practical challenges that arise in real computer investigations

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management solutions. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors’ respective areas of expertise. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader’s grasp of the material and ability to implement practical solutions

This textbook is for courses in cyber security education that follow National Initiative for Cybersecurity Education (NICE) KSAs work roles and framework, that adopt the Competency-Based Education (CBE) method. The book follows the CBT (KSA) general framework, meaning each chapter contains three sections, knowledge and questions, and skills/labs for Skills and Abilities. The author makes an explicit balance between knowledge and skills material in information security, giving readers immediate applicable skills. The book is divided into seven parts: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analysis; Operate and Collect; Investigate. All classroom materials (in the book an ancillary) adhere to the NICE framework. Mirrors classes set up by the National Initiative for Cybersecurity Education (NICE) Adopts the Competency-Based Education (CBE) method of teaching, used by universities, corporations, and in government training Includes content and ancillaries that provide skill-based instruction on compliance laws, information security standards, risk response and recovery, and more

Every year, in response to advancements in technology and new laws in different countries and regions, there are many changes and updates to the body of knowledge required of IT security professionals. Updated annually to keep up with the increasingly fast pace of change in the field, the Information Security Management Handbook is the single most

Today, security demands unprecedented visibility into your network. Cisco NetFlow can help companies of all sizes achieve and maintain this visibility. Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security is the definitive guide to using NetFlow to strengthen network security. Omar Santos, Technical Leader of Cisco's Product Security Incident Response Team (PSIRT), covers all you need to successfully capture network telemetry with NetFlow and use it to: See what is actually happening across your entire network Regain control of your network Quickly identify compromised end points and network infrastructure devices Monitor network usage by employees, contractors, or partners Detect firewall misconfigurations and inappropriate access to corporate resources Act effectively during incident response and network forensics Utilize big data analytics to improve IT security Writing for organizations of all sizes, Santos shows how to work with each current version of NetFlow, and several leading open source analyzers. He addresses NetFlow services, versions, and features; shows how to perform Big Data security analyses of Cisco NetFlow data; and explains how NetFlow integrates into broader Cisco Cyber Threat Defense (CTD) solutions. Each chapter presents multiple sample configurations, accompanied by detailed design analyses and realistic case studies.

A detailed and complete guide to exporting, collecting, analyzing, and understanding network flows to make managing networks easier. Network flow analysis is the art of studying the traffic on a computer network. Understanding the ways to export flow and collect and analyze data separates good network administrators from great ones. The detailed instructions in Network Flow Analysis teach the busy network administrator how to build every component of a flow-based network awareness system and how network analysis and auditing can help address problems and improve network reliability. Readers learn what flow is, how flows are used in network management, and how to use a flow analysis system. Real-world examples illustrate how to best apply the appropriate tools and how to analyze data to solve real problems. Lucas compares existing popular tools for network management, explaining why they don't address common real-world issues and demonstrates how, once a network administrator understands the underlying process and techniques of flow management, building a flow management system from freely-available components is not only possible but actually a better choice than much more expensive systems.

Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Dieses Dokument befasst sich mit CISCO NetFlow, dem NetFlow-Tool NFSen/NFDump und der in ACOnet bereits eingesetzten Software Arbor Peakflow SP. Das Dokument ist unterteilt in 5 Teile. Der erste Teil gibt einen Überblick über die aktuelle Netzwerk-Topologie in ACOnet und VIX, der zweite Teil befasst sich näher mit den eingesetzten Tools NFSen/NFDump und Peakflow. Im dritten Teil wird näher auf die Theorie zu CISCO NetFlow eingegangen, wie ein NetFlow entsteht, welche Versionen verwendet werden und welche Unterschiede in der Anwendung zwischen den einzelnen Versionen auftreten. Im vierten Teil des Dokumentes wird ein Security-Incidents mit Hilfe von NFSen/NFDump rekonstruiert. Der fünfte und letzte Teil befasst sich mit dem Vergleich der beiden vorher beschriebenen Tools auf die Einsatzmöglichkeiten und die Anwendbarkeit im Alltag eines Networksecurity-Beauftragten.

Expert solutions for securing network infrastructures and VPNs Build security into the network by defining zones, implementing secure routing protocol designs, and building safe LAN switching environments Understand the inner workings of the Cisco PIX Firewall and analyze in-depth Cisco PIX Firewall and Cisco IOS Firewall features and concepts Understand what VPNs are and how they are implemented with protocols such as GRE, L2TP, and IPSec Gain a packet-level understanding of the IPSec suite of protocols, its associated encryption and hashing functions, and authentication techniques Learn how network attacks can be categorized and how the Cisco IDS is designed and can be set upto protect against them Control network access by learning how AAA fits into the Cisco security model and by implementing RADIUS and TACACS+ protocols Provision service provider security using ACLs, NBAR, and CAR to identify and control attacks Identify and resolve common implementation failures by evaluating real-world troubleshooting scenarios As organizations increase their dependence on networks for core business processes and increase access to remote sites and mobile workers via virtual private networks (VPNs), network security becomes more and more critical. In today's networked era, information is an organization's most valuable resource. Lack of customer, partner, and employee access to e-commerce and data servers can impact both revenue and productivity. Even so, most networks do not have the proper degree of security. Network Security Principles and Practices provides an in-depth understanding of the policies, products, and expertise that brings organization to this extremely complex topic and boosts your confidence in the performance and integrity of your network systems and services. Written by the CCIE engineer who wrote the CCIE Security lab exam and who helped develop the CCIE Security written exam, Network Security Principles and Practices is the first book to help prepare candidates for the CCIE Security exams. Network Security Principles and Practices is a comprehensive guide to network security threats and the policies and tools developed specifically to combat those threats. Taking a practical, applied approach to building security into networks, the book shows you how to build secure network architectures from the ground up. Security aspects of routing protocols, Layer 2 threats, and switch security features are all analyzed. A comprehensive treatment of VPNs and IPSec is presented in extensive packet-by-packet detail. The book takes a behind-the-scenes look at how the Cisco PIX(r) Firewall actually works, presenting many difficult-to-understand and new Cisco PIX Firewall and Cisco IOS(r) Firewall concepts. The book launches into a discussion of intrusion detection systems (IDS) by analyzing and breaking down modern-day network attacks, describing how an IDS deals with those threats in general, and elaborating on the Cisco implementation of IDS. The book also discusses AAA, RADIUS, and TACACS+ and their usage with some of the newer security implementations such as VPNs and proxy authentication. A complete section devoted to service provider techniques for enhancing customer security and providing support in the event of an attack is also included. Finally, the book concludes with a section dedicated to discussing tried-and-tested troubleshooting tools and techniques that are not only invaluable to candidates working toward their CCIE Security lab exam but also to the security network administrator running the operations of a network on a daily basis.

Learn about network security, including the threats and the ways a network is protected from them. The book also covers firewalls, viruses and virtual private networks.

This new text provides students the knowledge and skills they will need to compete for and succeed in the information security roles they will encounter straight out of college. This is accomplished by providing a hands-on immersion in essential system administration, service and application installation and configuration, security tool use, TIG implementation and reporting. It is designed for an introductory course on IS Security offered usually as an elective in IS departments in 2 and 4 year schools. It is not designed for security certification courses.

This book constitutes the refereed proceedings of the 8th International Conference on Intelligent Computing, ICIC 2012, held in Huangshan, China, in July 2012. The 242 revised full papers presented in the three volumes LNCS 7389, LNAI 7390, and CCIS 304 were carefully reviewed and selected from 753 submissions. The papers in this volume (CCIS 304) are organized in topical sections on Neural Networks; Particle Swarm Optimization and Niche Technology; Kernel Methods and Supporting Vector Machines; Biology Inspired Computing and Optimization; Knowledge Discovery and Data Mining; Intelligent Computing in Bioinformatics; Intelligent Computing in Pattern Recognition; Intelligent Computing in Image Processing; Intelligent Computing in Computer Vision; Intelligent Control and Automation; Knowledge Representation/Reasoning and Expert Systems; Advances in Information Security; Protein and Gene Bioinformatics; Soft Computing and Bio-Inspired Techiques in Real-World Applications; Bio-Inspired Computing and Applications.

More than 6 hours of video training covering everything you need to know to deploy, configure, and troubleshoot NetFlow in many different Cisco platforms and learn big data analytics technologies for cyber security. Description Cisco NetFlow for Cyber Security Big Data Analytics walks you through the steps for deploying, configuring, and troubleshooting NetFlow and learning big data analytics technologies for cyber security. Cisco NetFlow creates an environment where network administrators and security professionals have the tools to understand who, what, when, where, and how network traffic is flowing. Cisco NetFlow LiveLessons is a key resource for understanding the power behind the Cisco NetFlow solution. Omar Santos, a Cisco Product Security Incident Response Team (PSIRT) technical leader and author of Network Security with NetFlow and IPFIX, the CCNA Security 210-260 Official Cert Guide, and other key security video and book titles by Cisco Press demonstrates how NetFlow can be used by large enterprises and small-to-medium-sized businesses to meet critical network challenges. This video courseexplores everything you need to understand and implement the Cisco Cyber Threat Defense Solution, while also providing configuration and troubleshooting walk-throughs. Skill Level Intermediate What You Will Learn NetFlow and IPFIX basics NetFlow Deployment Scenarios Cisco Flexible NetFlow NetFlow Commercial and Open Source Monitoring and Analysis Software Packages Big Data Analytics Tools The Cisco Cyber Threat Defense Solution Troubleshooting NetFlow NetFlow for Anomaly Detection and Identifying DoS Attacks NetFlow for Incident Response and Forensics Who Should Take This Course Network and security professionals interested in learning about the Cisco NetFlow solution; anyone wishing to build Cisco security About LiveLessons Video Training LiveLessons Video Training series publishes hundreds of hands-on, expert-led video tutorials covering a wide selection of technology topics designed to teach you the skills you need to succeed. This professional and personal technology video series features world-leading author instructors published by your trusted technology brands: Addison-Wesley, Cisco Press, IBM Press, Pearson IT Certification, Prentice Hall, Sams, and Que. Topics include: IT Certification, Programming, Web Development, Mobile Development, Home and Office Technologies, Business and Management, and more. View all LiveLessons on InformIT at http:...

This volume constitutes the refereed proceedings of the 13th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2019, held in Paris, France, in December 2019. The 12 full papers and 2 short papers presented were carefully reviewed and selected from 42 submissions. The papers are organized in the following topical sections: authentication; cryptography; threats; cybersecurity; and Internet of Things.

End-to-End Network Security Defense-in-Depth Best practices for assessing and improving network defenses and responding to security incidents Omar Santos Information security practices have evolved from Internet perimeter protection to an in-depth defense model in which multiple countermeasures are layered throughout the infrastructure to address vulnerabilities and attacks. This is necessary due to increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity--all blurring the boundaries between the network and perimeter. End-to-End Network Security is designed to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in your network. The ultimate goal is to deploy a set of security capabilities that together create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds. End-to-End Network Security provides you with a comprehensive look at the mechanisms to counter threats to each part of your network. The book starts with a review of network security technologies then covers the six-step methodology for incident response and best practices from proactive security frameworks. Later chapters cover wireless network security, IP telephony security, data center security, and IPv6 security. Finally, several case studies representing small, medium, and large enterprises provide detailed example configurations and implementation strategies of best practices learned in earlier chapters. Adopting the techniques and strategies outlined in this book enables you to prevent day-zero attacks, improve your overall security posture, build strong policies, and deploy intelligent, self-defending networks. "Within these pages, you will find many practical tools, both process related and technology related, that you can draw on to improve your risk mitigation strategies." --Bruce Murphy, Vice President, World Wide Security Practices, Cisco Omar Santos is a senior network security engineer at Cisco. Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations. Guard your network with firewalls, VPNs, and intrusion prevention systems Control network access with AAA Enforce security policies with Cisco Network Admission Control (NAC) Learn how to perform risk and threat analysis Harden your network infrastructure, security policies, and procedures against security threats Identify and classify security threats Trace back attacks to their source Learn how to best react to security incidents Maintain visibility and control over your network with the SAVE framework Apply Defense-in-Depth principles to wireless networks, IP telephony networks, data centers, and IPv6 networks This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: Network security and incident response

This book gathers peer-reviewed proceedings of the 3rd International Conference on Innovative Computing (IC 2020). This book aims to provide an open forum for discussing recent advances and emerging trends in information technology, science, and engineering. Themes within the scope of the conference include Communication Networks, Business Intelligence and Knowledge Management, Web Intelligence, and any related fields that depend on the development of information technology. The respective contributions presented here cover a wide range of topics, from databases and data mining, networking and communications, the web and Internet of Things, to embedded systems, soft computing, social network analysis, security and privacy, optical communication, and ubiquitous/pervasive computing. Readers such as students, researchers, and industry professionals in the fields of cloud computing, Internet of Things, machine learning, information security, multimedia systems, and information technology benefit from this comprehensive overview of the latest advances in information technology. The book can also benefit young investigators looking to start a new research program.

This book constitutes the proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS 2015, held as part of the 17th International Conference on Human-Computer Interaction, HCII 2015, held in Los Angeles, CA, USA, in August 2015 and received a total of 4843 submissions, of which 1462 papers and 246 posters were accepted for publication after a careful reviewing process. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers thoroughly cover the entire field of Human-Computer Interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. The 62 papers presented in the HAS 2015 proceedings are organized in topical sections as follows: authentication, cybersecurity, privacy, security, and user behavior, security in social media and smart technologies, and security technologies.

This book highlights several gaps that have not been addressed in existing cyber security research. It first discusses the recent attack prediction techniques that utilize one or more aspects of information to create attack prediction models. The second part is dedicated to new trends on information fusion and their applicability to cyber security; in particular, graph data analytics for cyber security, unwanted traffic detection and control based on trust management software defined networks, security in wireless sensor networks & their applications, and emerging trends in security system design using the concept of social behavioral biometric. The book guides the design of new commercialized tools that can be introduced to improve the accuracy of existing attack prediction models. Furthermore, the book advances the use of Knowledge-based Intrusion Detection Systems (IDS) to complement existing IDS technologies. It is aimed towards cyber security researchers.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Implementing Cisco IOS Network Security (IINS) is a Cisco-authorized, self-paced learning tool for CCNA® Security foundation learning. This book provides you with the knowledge needed to secure Cisco® routers and switches and their associated networks. By reading this book, you will gain a thorough understanding of how to troubleshoot and monitor network devices to maintain integrity, confidentiality, and availability of data and devices, as well as the technologies that Cisco uses in its security infrastructure. This book focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. You will learn how to perform basic tasks to secure a small branch type office network using Cisco IOS® security features available through the Cisco Router and Security Device Manager (SDM) web-based graphical user interface (GUI) and through the command-line interface (CLI) on Cisco routers and switches. The author also provides, when appropriate, parallels with Cisco ASA appliances. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco

Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. Develop a comprehensive network security policy to counter threats against information security Configure routers on the network perimeter with Cisco IOS Software security features Configure firewall features including ACLs and Cisco IOS zone-based policy firewalls to perform basic security operations on a network Configure site-to-site VPNs using Cisco IOS features Configure IPS on Cisco network routers Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic This volume is in the Certification Self-Study Series offered by Cisco Press®. Books in this series provide officially developed self-study solutions to help networking professionals understand technology implementations and prepare for the Cisco Career Certifications examinations.

Cyber-security is a matter of rapidly growing importance in industry and government. This book provides insight into a range of data science techniques for addressing these pressing concerns.The application of statistical and broader data science techniques provides an exciting growth area in the design of cyber defences. Networks of connected devices, such as enterprise computer networks or the wider so-called Internet of Things, are all vulnerable to misuse and attack, and data science methods offer the promise to detect such behaviours from the vast collections of cyber traffic data sources that can be obtained. In many cases, this is achieved through anomaly detection of unusual behaviour against understood statistical models of normality.This volume presents contributed papers from an international conference of the same name held at Imperial College. Experts from the field have provided their latest discoveries and review state of the art technologies.

This book constitutes the proceedings of the 5th International Symposium on Cyberspace Safety and Security, CSS 2013, held in Zhangjiajie, China, in November 2013. The 30 full papers presented in this volume were carefully reviewed and selected from 105 submissions. In addition the book contains 6 workshop papers. The papers are organized in topical sections named: data and applications security; network and communications security; software and systems security; and cloud security and cyberspace safety.

Traditional intrusion detection and logfile analysis are no longer enough to protect today’s complex networks. In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You’ll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. It’s ideal for network administrators and operational security analysts familiar with scripting. Explore network, host, and service sensors for capturing security data Store data traffic with relational databases, graph databases, Redis, and Hadoop Use SiLK, the R language, and other tools for analysis and visualization Detect unusual phenomena through Exploratory Data Analysis (EDA) Identify significant structures in networks with graph analysis Determine the traffic that’s crossing service ports in a network Examine traffic volume and behavior to spot DDoS and database raids Get a step-by-step process for network mapping and inventory

This complete new guide to auditing network security is an indispensable resource for security, network, and IT professionals, and for the consultants and technology partners who serve them. Cisco network security expert Chris Jackson begins with a thorough overview of the auditing process, including coverage of the latest regulations, compliance issues, and industry best practices. The author then demonstrates how to segment security architectures into domains and measure security effectiveness through a comprehensive systems approach. Network Security Auditing thoroughly covers the use of both commercial and open source tools to assist in auditing and validating security policy assumptions. The book also introduces leading IT governance frameworks such as COBIT, ITIL, and ISO 17799/27001, explaining their values, usages, and effective integrations with Cisco security products.

This book constitutes the refereed proceedings of the 12th International Conference on Cryptology and Network Security, CANS 2013, held in Paraty, Brazil, in November 2013. The 18 revised full papers presented together with four invited talks were carefully reviewed and selected from 57 submissions. The papers are organized in topical sections on cryptanalysis, zero-knowledge protocols, distributed protocols, network security and applications, advanced cryptographic primitives, and verifiable computation.

Network Security With Netflow and IpfixBig Data Analytics for Information SecurityCisco Systems

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM. Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster. The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data. If you've never performed NSM analysis, Applied Network Security Monitoring will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job. Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples Companion website includes up-to-date blogs from the authors about the latest developments in NSM

This book presents the set of papers accepted for presentation at the International Conference Automation, held in Warsaw, 2-4 March of 2016. It presents the research results presented by top experts in the fields of industrial automation, control, robotics and measurement techniques. Each chapter presents a thorough analysis of a specific technical problem which is usually followed by numerical analysis, simulation, and description of results of implementation of the solution of a real world problem. The presented theoretical results, practical solutions and guidelines will be valuable for both researchers working in the area of engineering sciences and for practitioners solving industrial problems.

This book constitutes the refereed proceedings of the workshops held at the 16th Asia-Pacific Web Conference, APWeb 2014, in Changsha, China, in September 2014. The 34 full papers were carefully reviewed and selected from 59 submissions. This volume presents the papers that have been accepted for the following workshops: First International Workshop on Social Network Analysis, SNA 2014; First International Workshop on Network and Information Security, NIS 2014; First International Workshop on Internet of Things Search, IoTS 2014. The papers cover various issues in social network analysis, security and information retrieval against the heterogeneous big data.

"Cisco NetFlow for Cyber Security Big Data Analytics walks you through the steps for deploying, configuring, and troubleshooting NetFlow and learning big data analytics technologies for cyber security. Cisco NetFlow creates an environment where network administrators and security professionals have the tools to understand who, what, when, where, and how network traffic is flowing. Cisco NetFlow LiveLessons is a key resource for understanding the power behind the Cisco NetFlow solution."--Resource description page.

Welcome to the Third International Conference on Information Security and Ass- ance (ISA 2009). ISA 2009 was the most comprehensive conference focused on the various aspects of advances in information security and assurance. The concept of security and assurance is emerging rapidly as an exciting new paradigm to provide reliable and safe life services. Our conference provides a chance for academic and industry professionals to discuss recent progress in the area of communication and networking including modeling, simulation and novel applications associated with the utilization and acceptance of computing devices and systems. ISA 2009 was a succ- sor of the First International Workshop on Information Assurance in Networks (IAN 2007, Jeju-island, Korea, December, 2007), and the Second International Conference on Information Security and Assurance (ISA 2008, Busan, Korea, April 2008). The goal of this conference is to bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of information technology. ISA 2009 contained research papers submitted by researchers from all over the world. In order to guarantee high-quality proceedings, we put extensive effort into reviewing the papers. All submissions were peer reviewed by at least three Program Committee members as well as external reviewers. As the quality of the submissions was quite high, it was extremely difficult to select the papers for oral presentation and publication in the proceedings of the conference.

Provides information on the basics of computer network security, covering such topics as hackers, security policies, security technologies, firewalls, routers, VPNs, wireless security, and honeypots.

Updated annually to keep up with the increasingly fast pace of change in the field, the Information Security Management Handbook is the single most comprehensive and up-to-date resource on information security (IS) and assurance. Facilitating the up-to-date understanding required of all IS professionals, the Information Security Management Handbook

Every year, in response to new technologies and new laws in different countries and regions, there are changes to the fundamental knowledge, skills, techniques, and tools required by all IT security professionals. In step with the lightning-quick, increasingly fast pace of change in the technology field, the Information Security Management Handbook, updated yearly, has become the standard on which all IT security programs and certifications are based. It reflects new updates to the Common Body of Knowledge (CBK) that IT security professionals all over the globe need to know. Captures the crucial elements of the CBK Exploring the ten domains of the CBK, the book explores access control, telecommunications and network security, information security and risk management, application security, and cryptography. In addition, the expert contributors address security architecture and design, operations security, business continuity planning and disaster recovery planning. The book also covers legal regulations, compliance, investigation, and physical security. In this anthology of treatises dealing with the management and technical facets of information security, the contributors examine varied topics such as anywhere computing, virtualization, podslurping, quantum computing, mashups, blue snarfing, mobile device theft, social computing, voting machine insecurity, and format string vulnerabilities. Also available on CD-ROM Safeguarding information continues to be a crucial concern of all IT professionals. As new risks threaten the security of our systems, it is imperative that those charged with protecting that information continually update their armor of knowledge to guard against tomorrow’s hackers and software vulnerabilities. This comprehensive Handbook, also available in fully searchable CD-ROM format keeps IT professionals abreast of new developments on the security horizon and reinforces timeless concepts, providing them with the best information, guidance, and counsel they can obtain.

Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

A definitive how-to guide to the Cisco security blueprint examines a wide variety of security issues and concepts, furnishes a broad overview of the ins and outs of implementing a comprehensive security plan--from identifying security threats to defending a network--and discusses specific solutions to a variety of security problems. (Beginner)

As an under-studied area of academic research, the analysis of computer network traffic data is still in its infancy. However, the challenge of detecting and mitigating malicious or unauthorised behaviour through the lens of such data is becoming an increasingly prominent issue. This collection of papers by leading researchers and practitioners synthesises cutting-edge work in the analysis of dynamic networks and statistical aspects of cyber security. The book is structured in such a way as to keep security application at the forefront of discussions. It offers readers easy access into the area of data analysis for complex cyber-security applications, with a particular focus on temporal and network aspects. Chapters can be read as standalone sections and provide rich reviews of the latest research within the field of cyber-security. Academic readers will benefit from state-of-the-art descriptions of new methodologies and their extension to real practical problems while industry professionals will appreciate access to more advanced methodology than ever before. Contents:Network Attacks and the Data They Affect (M Morgan, J Sexton, J Neil, A Ricciardi & J Theimer)Cyber-Security Data Sources for Dynamic Network Research (A D Kent)Modelling User Behaviour in a Network Using Computer Event Logs (M J M Turcotte, N A Heard & A D Kent)Network Services as Risk Factors: A Genetic Epidemiology Approach to Cyber-Security (S Gil)Community Detection and Role Identification in Directed Networks: Understanding the Twitter Network of the Care.Data Debate (B Amor, S Vuik, R Callahan, A Darzi, S N Yaliraki & M Barahona)Anomaly Detection for Cyber Security Applications (P Rubin-Delanchy, D J Lawson & N A Heard)Exponential Random Graph Modelling of Static and Dynamic Social Networks (A Caimo)Hierarchical Dynamic Walks (A V Mantzaris, P Grindrod & D J Higham)Temporal Reachability in Dynamic Networks (A Hagberg, N Lemons & S Misra) Readership: Researchers and practitioners in dynamic network analysis and cyber-security. Key Features:Detailed descriptions of the behaviour of attackersDiscussions of new public domain data sources, including data quality issuesA collection of papers introducing novel methodology for cyber-data analysis