Network Defense Security Policy And Threats Ec Council Press

Eventually, you will extremely discover a supplementary experience and achievement by spending more cash. nevertheless when? get you take on that you require to get those every needs later than having significantly cash? Why dont you attempt to get something basic in the beginning? Thats something that will guide you to comprehend even more on the globe, experience, some places, in the same way as history, amusement, and a lot more?

It is your unquestionably own period to statute reviewing habit. in the midst of guides you could enjoy now is **Network Defense Security Policy And Threats Ec Council Press** below.

The Nordic Countries and the European Security and Defence Policy - Alyson J. K. Bailes 2006
In 1999 the EU decided to develop its own military capacities for crisis management. This book brings together a group of experts to examine the consequences of this decision on Nordic policy establishments, as well as to shed new light on the defence and security issues that matter for Europe as a whole.
Security and Defence in Europe - J. Martín Ramírez 2019-05-24
This book argues that security and defense have never been true priorities in the European Union, and have constantly been marginalized by the elites since the Soviet Union collapsed and the Warsaw Pact disintegrated. Despite the official rhetoric, only a few tangible results can be presented concerning the operational readiness of European forces, and the EU's inability to act was proven during the crises in the Balkans, NATO has experienced similar problems, as the majority of its members are EU countries. Both organizations have declared their resolve concerning the security and defense of their nations and territories, but, unfortunately, little has been done to lend these statements credence. In this context, the book analyzes several aspects of EU security and defense, including: the EU – NATO relationship, common defense policy and strategy, common capability building, common understanding of strategic changes, common operational planning and centrally synchronized exercises based on operational planning, etc. The member states have helped to make EU/NATO effective organizations, but unfortunately their individual interests and priorities constitute real challenges. This aspect should be discussed and addressed by political and military elites, scholars, analysts, students and the general public alike.
Computers at Risk - National Research Council 1990-02-01
Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.
Effective Model-Based Systems Engineering - John M. Borky 2018-09-08
This textbook presents a proven, mature Model-Based Systems Engineering (MBSE) methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the

practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices that furnish additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.

Ethical Hacking and Countermeasures: Web Applications and Data Servers - EC-Council 2009-09-24

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention - Dhavale, Sunita Vikrant 2018-12-14

In recent decades there has been incredible growth in the use of various internet applications by individuals and organizations who store sensitive information online on different servers. This greater reliance of organizations and individuals on internet technologies and applications increases the threat space and poses several challenges for implementing and maintaining cybersecurity practices. Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention provides innovative insights into how an ethical hacking knowledge base can be used for testing and improving the network and system security posture of an organization. It is critical for each individual and institute to learn hacking tools and techniques that are used by dangerous hackers in tandem with forming a team of ethical hacking professionals to test their systems effectively. Highlighting topics including cyber operations, server security, and network statistics, this publication is designed for technical experts, students, academicians, government officials, and industry professionals.

Cyber Security Policy Guidebook - Jennifer L. Bayuk 2012-04-24

Drawing upon a wealth of experience from academia, industry, and government service, Cyber Security Policy Guidebook details and dissects, in simple language, current organizational cyber security policy issues on a global scale—taking great care to educate readers on the history and current approaches to the security of cyberspace. It includes thorough descriptions—as well as the pros and cons—of a plethora of issues, and documents policy alternatives for the sake of clarity with respect to policy alone. The Guidebook also delves into organizational implementation issues, and equips readers with descriptions of the positive and negative impact of specific policy choices. Inside are detailed chapters that: Explain what is meant by cyber security and cyber security policy Discuss the process by which cyber security policy goals are set Educate the reader on decision-making processes related to cyber security Describe a new framework and taxonomy for explaining cyber security policy issues Show how the U.S. government is dealing with cyber security policy issues With a glossary that puts cyber security language in layman's terms—and diagrams that help explain complex topics—Cyber Security Policy Guidebook gives students, scholars, and technical decision-makers the necessary knowledge to make informed decisions on cyber security policy.

Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications - Management Association, Information Resources 2018-05-04

Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems - EC-Council 2009-09-24

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cyber Security: Threats and Responses for Government and Business - Jack Caravelli 2019-02-22

This timely and compelling book presents a broad study of all key cyber security issues of the highest interest to government and business as well as their implications. • Takes a broad approach to the problems of cyber security, covering every important issue related to the threats cyber security poses to government and business • Provides detailed coverage of the political, financial, data protection, privacy, and reputational problems caused by cyber attacks • Offers a forward-looking approach, discussing emerging trends that will bring new challenges to those charged with enhancing cyber security • Makes insightful suggestions into how nations and businesses can take steps to enhance their cyber security

EU Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Regulations - IBP, Inc. 2013-07-01

EU National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments

Research Handbook on Information Law and Governance - Sandeen, Sharon K. 2021-09-23

This fresh and insightful Research Handbook delivers global perspectives on information law and governance, delving into principles of information law in the areas of trade secrecy, privacy, data protection and cybersecurity.

Network Defense: Securing and Troubleshooting Network Operating Systems - EC-Council 2010-04-14

The Network Defense Series from EC-Council | Press is comprised of 5 books designed to educate learners from a vendor-neutral standpoint how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security and design, how to enforce network level security policies, and how to ultimately protect an organization's information. The books in the series cover a broad range of topics from secure network fundamentals, protocols & analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS, firewalls, bastion host and honeypots. Learners completing this series will have a full understanding of defensive measures taken to secure their organization's information, and along with the proper experience these books will prepare readers for the EC-Council Network Security Administrator (E|NSA) certification. Unpatched software on network operating systems and hardware can be a common point of attack for an intruder. Vulnerability analysis will often identify outdated software and exploitation is soon to follow. This book, the fourth in the series, prepares the practitioner to create and administer effective policies and best practices in patch management, OS configuration and analysis to identify potential Network Security Weaknesses. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Network Defense: Fundamentals and Protocols - EC-Council 2010-03-29

The Network Defense Series from EC-Council | Press is comprised of 5 books designed to educate learners from a vendor-neutral standpoint how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security and design, how to enforce network level security policies, and how to ultimately protect an organization's information. The books in the series cover a broad range of topics from secure network fundamentals, protocols & analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS, firewalls, bastion host and honeypots. Learners completing this series will have a full understanding of defensive measures taken to secure their organization's information, and along with the proper experience these books will prepare readers for the EC-Council Network Security Administrator (E|NSA) certification. A thorough understanding of network technologies and security fundamentals is required before designing any defensive measure to protect an organization's information. This book, the first in the series, is designed to provide the foundational knowledge to the potential Security Administrator from a vendor-neutral perspective covering everything from standard secure network topology, network media and transmission, classifications, and a complete view of network security equipment. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Identity Theft: Breakthroughs in Research and Practice - Management Association, Information Resources 2016-09-27

The preservation of private data is a main concern of governments, organizations, and individuals alike. For individuals, a breach in personal information can mean dire consequences for an individual’s finances, medical information, and personal property. Identity Theft: Breakthroughs in Research and Practice highlights emerging perspectives and critical insights into the preservation of personal data and the complications that can arise when one’s identity is compromised. This critical volume features key research on methods and technologies for protection, the problems associated with identity theft, and outlooks for the future. This publication is an essential resource for information security professionals, researchers, and graduate-level students in the fields of criminal science, business, and computer science.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked world -

Research Handbook on the EU’s Common Foreign and Security Policy - Steven

Blockmans 2018
In times of rapid change and unpredictability the European Union's role in the world is sorely tested. How successfully the EU meets challenges such as war, terrorism and climate change, and how effectively the Union taps into opportunities like mobility and technological progress depends to a great extent on the ability of the EU's institutions and member states to adopt and implement a comprehensive and integrated approach to external action. This Research Handbook examines the law, policy and practice of the EU's Common Foreign and Security Policy, including the Common Security and Defence, and gauges its interactions with the other external policies of the Union (including trade, development, energy), as well as the evolving political and economic challenges that face the European Union.

Electronic Commerce 2018 - Efraim Turban 2017-10-12
This new Edition of Electronic Commerce is a complete update of the leading graduate level/advanced undergraduate level textbook on the subject. Electronic commerce (EC) describes the manner in which transactions take place over electronic networks, mostly the Internet. It is the process of electronically buying and selling goods, services, and information. Certain EC applications, such as buying and selling stocks and airline tickets online, are reaching maturity, some even exceeding non-Internet trades. However, EC is not just about buying and selling; it also is about electronically communicating, collaborating, and discovering information. It is about e-learning, e-government, social networks, and much more. EC is having an impact on a significant portion of the world, affecting businesses, professions, trade, and of course, people. The most important developments in EC since 2014 are the continuous phenomenal growth of social networks, especially Facebook , LinkedIn and Instagram, and the trend toward conducting EC with mobile devices. Other major developments are the expansion of EC globally, especially in China where you can find the world's largest EC company. Much attention is lately being given to smart commerce and the use of AI-based analytics and big data to enhance the field. Finally, some emerging EC business models are changing industries (e.g., the shared economy models of Uber and Airbnb). The 2018 (9th) edition, brings forth the latest trends in e-commerce, including smart commerce, social commerce, social collaboration, shared economy, innovations, and mobility.

Toward Effective Cyber Defense in Accordance with the Rules of Law - A. Brill 2020-06-18
Information and communication technologies now play a big part in the daily personal and professional lives of us all. Cyberspace – the interconnected digital technology domain which underlies communications, transportation, state administration, finance, medicine and education – is part of all our lives. In the last decade, the digital revolution in the South Eastern European (SEE) countries has given more people there access to communication, education, and news than ever before, and we should not underestimate the power of these information and communication technologies. This book presents papers from the NATO Science for Peace and Security Advanced Training Course (ATC) Toward Effective Cyber Defense in Accordance With the Rules of Law, held in Ohrid, Republic of North Macedonia, in November 2019. The course focused on the SEE countries, where, in general, governments have paid appropriate attention to developing cyber defense capacities. In some cases, however, limitations in technological resources have restricted the capabilities of governments to respond to the ever-evolving challenges of defending the cyber domain. Laws and regulations differ from country to country, and the topics covered here were carefully chosen to cover issues in laws and regulations, cyber defense policies and their practical implementation. The series of papers presented in this book will provide a deeper understanding of these topics for scholars, associated professionals in the public and private sectors, and for a more general audience.

Cyberspace - J. Martín Ramírez 2017-05-11
This book covers many aspects of cyberspace, emphasizing not only its possible 'negative' challenge as a threat to security, but also its positive influence as an efficient tool for defense as well as a welcome new factor for economic and industrial production. Cyberspace is analyzed from quite different and

interdisciplinary perspectives, such as: conceptual and legal, military and socio-civil, psychological, commercial, cyber delinquency, cyber intelligence applied to public and private institutions, as well as the nuclear governance.

Cybersecurity – Attack and Defense Strategies - Yuri Diogenes 2019-12-31

Updated and revised edition of the bestselling guide to developing defense strategies against the latest threats to cybersecurity Key FeaturesCovers the latest security threats and defense strategies for 2020Introduces techniques and skillsets required to conduct threat hunting and deal with a system breachProvides new information on Cloud Security Posture Management, Microsoft Azure Threat Protection, Zero Trust Network strategies, Nation State attacks, the use of Azure Sentinel as a cloud-based SIEM for logging and investigation, and much moreBook Description Cybersecurity – Attack and Defense Strategies, Second Edition is a completely revised new edition of the bestselling book, covering the very latest security threats and defense mechanisms including a detailed overview of Cloud Security Posture Management (CSPM) and an assessment of the current threat landscape, with additional focus on new IoT threats and cryptomining. Cybersecurity starts with the basics that organizations need to know to maintain a secure posture against outside threat and design a robust cybersecurity program. It takes you into the mindset of a Threat Actor to help you better understand the motivation and the steps of performing an actual attack – the Cybersecurity kill chain. You will gain hands-on experience in implementing cybersecurity using new techniques in reconnaissance and chasing a user’s identity that will enable you to discover how a system is compromised, and identify and then exploit the vulnerabilities in your own system. This book also focuses on defense strategies to enhance the security of a system. You will also discover in-depth tools, including Azure Sentinel, to ensure there are security controls in each network layer, and how to carry out the recovery process of a compromised system. What you will learnThe importance of having a solid foundation for your security postureUse cyber security kill chain to understand the attack strategyBoost your organization’s cyber resilience by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligenceUtilize the latest defense tools, including Azure Sentinel and Zero Trust Network strategyIdentify different types of cyberattacks, such as SQL injection, malware and social engineering threats such as phishing emailsPerform an incident investigation using Azure Security Center and Azure SentinelGet an in-depth understanding of the disaster recovery processUnderstand how to consistently monitor security and implement a vulnerability management strategy for on-premises and hybrid cloud Learn how to perform log analysis using the cloud to identify suspicious activities, including logs from Amazon Web Services and AzureWho this book is for For the IT professional venturing into the IT security domain, IT pentesters, security consultants, or those looking to perform ethical hacking. Prior knowledge of penetration testing is beneficial.

The EU's Power in Inter-Organisational Relations - Hanna Ojanen 2017-11-28

This book studies inter-organisational relations from a new angle: power. Drawing on examples that highlight how the EU relates to NATO and to the UN, it shows how consequential inter-organisational relations are for the functioning and nature of the organisations, and how important it is to detect the forms of power exerted in these relations. Power, for international organisations, is above all about relevance. In an era when the legitimacy and role of international organisations is increasingly questioned, the organisations have a growing concern for ensuring their continued relevance. Subsequently, the management of relevance is a central part of inter-organisational relations and becomes visible in the way organisations handle questions about their tasks, hierarchies and image. Clear and accessible, the book will appeal both to the growing scholarly community working on inter-organisational relations and to a variety of audiences including practitioners and scholars outside the field of international relations.

Cybersecurity ??? Attack and Defense Strategies - Yuri Diogenes 2018-01-30

Enhance your organization’s secure posture by improving your attack and defense strategies

Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Ethical Hacking and Countermeasures: Threats and Defense Mechanisms - EC-Council 2016-03-17

The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Best Practices in Computer Network Defense: Incident Detection and Response - M. Hathaway 2014-01-21

The cyber security of vital infrastructure and services has become a major concern for countries worldwide. The members of NATO are no exception, and they share a responsibility to help the global community to strengthen its cyber defenses against malicious cyber activity. This book presents 10 papers and 21 specific findings from the NATO Advanced Research Workshop (ARW) ‘Best Practices in Computer Network Defense (CND): Incident Detection and Response, held in Geneva, Switzerland, in September 2013. The workshop was attended by a multi-disciplinary team of experts from 16 countries and three international institutions. The book identifies the state-of-the-art tools and processes being used for cyber defense and highlights gaps in the technology. It presents the best practice of industry and government for incident detection and response and examines indicators and metrics for progress along the security continuum.This book provides those operators and decision makers whose work it is to strengthen the cyber defenses of the global community with genuine tools and expert advice. Keeping pace and deploying advanced process or technology is only possible when you know what is available. This book shows what is possible and available today for computer network defense and for incident detection and response.

Developments and Advances in Defense and Security - Álvaro Rocha 2020-05-08

This book gathers the proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS), held at the Eloy Alfaro Military Academy (ESMIL) in Quito, Ecuador, on May 13–15,2020. It covers a broad range of topics in systems, communication, and defense; strategy and political–administrative vision in defense; and engineering and technologies applied to defense. Given its scope, it offers a valuable resource for practitioners, researchers, and students alike.

EU–Korea Security Relations - Nicola Casarini 2021-02-25

This book provides an original examination of current European Union (EU)–Republic of Korea (ROK) security relations. It brings together analysis and original material on relations in the fields of Nuclear non-proliferation and disarmament, Cybersecurity and data-protection, Space policy and technology, and Preventive diplomacy and crisis management. These represent areas of particular interest to examine the extent to which the EU and ROK are able to successfully or otherwise cooperate. Relations between the EU and the ROK have been growing in quantity and quality over recent years. Alongside the economic dimension, the political and security elements of the relationship have shown promise for further collaboration between the two sides, not least within the context of North Korea’s nuclear threat and East Asia’s wider evolving security environment. All contributors are leading experts in their respective fields and each chapter is co-authored by a European and Korean expert for a balanced assessment. The volume will be essential reading for students, scholars and policy-makers interested in EU–Korea relations, EU foreign policy and security, Area studies, and, more broadly to EU politics studies, security studies, and international relations.

Introduction to Electronic Commerce and Social Commerce - Efraim Turban 2017-04-23

This is a complete update of the best-selling undergraduate textbook on Electronic Commerce (EC). New to this 4th Edition is the addition of material on Social Commerce (two chapters); a new tutorial on the major EC support technologies, including cloud computing, RFID, and EDI; ten new learning outcomes; and video exercises added to most chapters. Wherever appropriate, material on Social Commerce has been added to existing chapters. Supplementary material includes an Instructor’s Manual; Test Bank questions for each chapter; Powerpoint Lecture Notes; and a Companion Website that includes EC support technologies as well as online files. The book is organized into 12 chapters grouped into 6 parts. Part 1 is an Introduction to E-Commerce and E-Marketplaces. Part 2 focuses on EC Applications, while Part 3 looks at Emerging EC Platforms, with two new chapters on Social Commerce and Enterprise Social Networks. Part 4 examines EC Support Services, and Part 5 looks at E-Commerce Strategy and Implementation. Part 6 is a collection of online tutorials on Launching Online Businesses and EC Projects, with tutorials focusing on e-CRM; EC Technology; Business Intelligence, including Data-, Text-, and Web Mining; E-Collaboration; and Competition in Cyberspace. the following="" tutorials="" are="" not="" related="" to="" any="" specific="" chapter.="" they="" cover="" the="" essentials="" ec="" technologies="" and="" provide="" a="" guide="" relevant="" resources.="" p

Network Defense and Countermeasures - William (Chuck) Easttom, II 2013

Network Defense and Countermeasures: Principles and Practices Everything you need to know about modern network attacks and defense, in one book Clearly explains core network security concepts, challenges, technologies, and skills Thoroughly updated for the latest attacks and countermeasures The perfect beginner''s guide for anyone interested in a network security career Security is the IT industry''s hottest topic-and that''s where the hottest opportunities are, too. Organizations desperately need professionals who can help them safeguard against the most sophisticated attacks ever created-attacks from well-funded global criminal syndicates, and even governments. Today, security begins with defending the organizational network. Network Defense and Countermeasures, Second Edition is today''s most complete, easy-to-understand introduction to modern network attacks and their effective defense. From malware and DDoS attacks to firewalls and encryption, Chuck Easttom blends theoretical foundations with up-to-the-minute best-practice techniques. Starting with the absolute basics, he discusses crucial topics many security books overlook, including the emergence of network-based espionage and terrorism. If you have a basic understanding of networks, that''s all the background you''ll need to succeed with this book: no math or advanced computer science is required. You''ll find projects, questions, exercises, case studies, links to expert resources, and a complete glossary-all designed to deepen your understanding and prepare you to defend real-world networks. Chuck Easttom has worked in all aspects of IT, including network administration, software engineering, and IT management. For several years, he has taught IT topics in college and corporate environments, worked as an independent IT consultant, and served as an expert witness in court cases involving computers. He holds 28 industry certifications, including CISSP, ISSAP, Certified Ethical Hacker, Certified Hacking Forensics Investigator, EC Council Certified Security Administrator, and EC Council Certified Instructor. He served as subject matter expert for CompTIA in its development or revision of four certification tests, including Security+. He recently assisted the EC Council in developing its new advanced cryptography course. Easttom has authored 13 books on topics including computer security and crime. Learn how to n Understand essential network security concepts, challenges, and careers n Learn how modern attacks work n Discover how firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) combine to protect modern networks n Select the right security technologies for any network environment n Use encryption to protect information n Harden Windows and Linux systems and keep them patched n Securely configure web browsers to resist attacks n Defend against malware n Define practical, enforceable security policies n Use the "6 Ps" to assess technical and human aspects of system security n Detect and fix system vulnerability n Apply proven security standards and models, including Orange Book, Common Criteria, and Bell-LaPadula n Ensure physical security and prepare for disaster recovery n Know your enemy: learn basic hacking, and see how to counter it n Understand standard forensic techniques and prepare for investigations of digital crime

Collaborative Cyber Threat Intelligence - Florian Skopik 2017-10-16

Threat intelligence is a surprisingly complex topic that goes far beyond the obvious technical challenges of collecting, modelling and sharing technical indicators. Most books in this area focus mainly on technical measures to harden a system based on threat intel data and limit their scope to single organizations only. This book provides a unique angle on the topic of national cyber threat intelligence and security information sharing. It also provides a clear view on ongoing works in research laboratories world-wide in order to address current security concerns at national level. It allows practitioners to learn about upcoming trends, researchers to share current results, and decision makers to prepare for future developments.

11th International Conference on Cyber Warfare and Security - Dr Tanya Zlateva and Professor Virginia Greiman 2016

The 11thInternational Conference on Cyber Warfare and Security (ICCWS 2016) is being held at Boston University, Boston, USA on the 17-18th March 2016. The Conference Chair is Dr Tanya Zlateva and the Programme Chair is Professor Virginia Greiman, both from Boston University. ICCWS is a recognised Cyber Security event on the International research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyber Warfare and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and expanding range of Cyberwar and

Cyber Security research available to them. The keynote speakers for the conference are Daryl Haegley from the Department of Defense (DoD), who will address the topic Control Systems Networks...What's in Your Building? and Neal Ziring from the National Security Agency who will be providing some insight to the issue of Is Security Achievable? A Practical Perspective. ICCWS received 125 abstract submissions this year. After the double blind, peer review process there are 43 Academic Research Papers 8 PhD papers Research papers, 7 Masters and 1 work-in-progress papers published in these Conference Proceedings. These papers represent work from around the world, including: Australia, Canada, China, Czech Republic, District of Columbia, Finland, France, Israel, Japan, Lebanon, Netherlands, Pakistan, Russian Federation, Saudi Arabia, South Africa, Turkey, United Arab Emirates, UK, USA.

At the Nexus of Cybersecurity and Public Policy - National Research Council 2014-06-16

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Employing Recent Technologies for Improved Digital Governance - Ponnusamy, Vasaki 2019-12-27

The digital divide, caused by several factors such as poverty and slow communication technologies, has offset the progression of many developing countries. However, with rapid changes in technology, a better collaboration among communities and governance based on the latest research in ICT and technology has begun to emerge. Employing Recent Technologies for Improved Digital Governance is an essential reference source that provides research on recent advances in the development, application, and impact of technologies for the initiative of digital governance. The book has a dual objective with the first objective being to encourage more research in deploying recent trends in the internet for deploying a collaborative digital governance. The second objective is to explore new possibilities using internet of things (IoT) and cloud/fog-based solutions for creating a collaboration between the governance and IT infrastructure. Featuring research on topics such as intelligent systems, social engineering, and cybersecurity, this book is ideally designed for policymakers, government officials, ICT specialists, researchers, academicians, industry professionals, and students.

Electronic Commerce - Efraim Turban 2015-01-29

Throughout the book, theoretical foundations necessary for understanding Electronic Commerce (EC) are presented, ranging from consumer behavior to the economic theory of competition. Furthermore, this book presents the most current topics relating to EC as described by a diversified team of experts in a variety of fields, including a senior vice president of an e-commerce-related company. The authors provide website resources, numerous exercises, and extensive references to supplement the theoretical presentations. At the end of each chapter, a list of online resources with links to the websites is also provided. Additionally, extensive, vivid examples from large corporations, small businesses from different industries, and services, governments, and nonprofit agencies from all over the world make concepts come alive in Electronic Commerce. These examples, which were collected by both academicians and practitioners, show the reader the capabilities of EC, its cost and justification, and the innovative ways corporations are using EC in their operations. In this edition (previous editions published by Pearson/Prentice Hall), the authors bring forth the latest trends in e-commerce, including social businesses, social networking, social collaboration, innovations, and mobility.

The EU, Strategy and Security Policy - Laura Chappell 2016-05-26

This edited collection is a timely and in-depth analysis of the EU’s efforts to bring coherency and strategy to its security policy actions. Despite a special European Council summit in December 2013 on defence, it is generally acknowledged that fifteen years since its inception the EU’s Common Security and Defence Policy (CSDP) has yet to acquire a clear sense of purpose. This book investigates those areas where the EU has established actorness in the security and defence field and asks whether they might constitute the elements of an emergent more coherent EU strategy on security. Taking a critical view, the contributors map the EU’s strategic vision(s) across particular key regions where the EU has been active as a security actor, the strategic challenges that it has pinpointed alongside the opportunities and barriers posed by a multiplicity of actors, interests and priorities identified by both member states and EU actors. By doing this we demonstrate where gaps in strategic thinking lie, where the EU has been unable to achieve its aims, and offer recommendations concerning the EU’s future strategic direction. This book will be of much interest to students of European security, EU policy, strategic studies and IR in general.

Taiwan Information Strategy, Internet and E-commerce Development Handbook - Strategic Information, Regulations, Contacts - IBP, Inc. 2016-09-08

Taiwan Information Strategy, Internet and E-Commerce Development Handbook - Strategic Information, Programs, Regulations

Cyber Defense - Policies, Operations and Capacity Building - S. Gaycken 2019-10-16

Besides becoming more complex, destructive, and coercive, military cyber threats are now ubiquitous, and it is difficult to imagine a future conflict that would not have a cyber dimension. This book presents the proceedings of CYDEF2018, a collaborative workshop between NATO and Japan, held in Tokyo, Japan, from 3 – 6 April 2018 under the umbrella of the NATO Science for Peace and Security Programme. It is divided into 3 sections: policy and diplomacy; operations and technology; and training and education, and covers subjects ranging from dealing with an evolving cyber threat picture to maintaining a skilled cyber workforce. The book serves as a unique reference for some of the most pressing challenges related to the implementation of effective cyber defense policy at a technical and operational level, and will be of interest to all those working in the field of cybersecurity.

Cyber Security in Parallel and Distributed Computing - Dac-Nhuong Le 2019-04-16

The book contains several new concepts, techniques, applications and case studies for cyber securities in parallel and distributed computing The main objective of this book is to explore the concept of cybersecurity in parallel and distributed computing along with recent research developments in the field. Also included are various real-time/offline applications and case studies in the fields of engineering and computer science and the modern tools and technologies used. Information concerning various topics relating to cybersecurity technologies is organized within the sixteen chapters of this book. Some of the important topics covered include: Research and solutions for the problem of hidden image detection Security aspects of data mining and possible solution techniques A comparative analysis of various methods used in e-commerce security and how to perform secure payment transactions in an efficient manner Blockchain technology and how it is crucial to the security industry Security for the Internet of Things Security issues and challenges in distributed computing security such as heterogeneous computing, cloud computing, fog computing, etc. Demonstrates the administration task issue in unified cloud situations as a multi-target enhancement issue in light of security Explores the concepts of cybercrime and cybersecurity and presents the statistical impact it is having on organizations Security policies and mechanisms, various categories of attacks (e.g., denial-of-service), global security architecture, along with distribution of security mechanisms Security issues in the healthcare sector with existing solutions and emerging threats.

The Emergence of EU Defense Research Policy - Nikolaos Karampekios 2017-11-16

This book explores European security and defense R&D policy, unveiling the strategic, industrial, institutional and ideational sources of the European Commission’s military research initiative. Starting from a well-defined empirical epicentre—the rise of non-civilian R&D priorities in the European Union—this book covers interrelated themes and topics such as approaches to arms production and R&D collaboration relationships between European R&D-related institutions technology and research foundations of European security policy past and present European armament collaborations transatlantic R&D collaboration the militarization of border security. Divided into 5 sections, the enclosed chapters explore the EU technology and innovation policy in regards to security, industrial competitiveness and military capabilities. The terrorist attacks in the US on September 11, 2001 provided a window of opportunity for the introduction of security as a distinct European R&D priority. In fact, since 2002, the Preparatory Action for Security Research (PASR) has funded 45 million euros to 39 research consortia to conduct security R&D. While the idea of pooling defense research efforts and programmes in Europe is not new, the establishment of institutions like the European Defense Agency (EDA) are a major step into institutionalizing European agencies involvement in supporting defense technology research. It is against this backdrop of policy developments that this book is positioned, in addition to addressing some of the political, economic, industrial and philosophical questions that arise. Featuring contributions from a variety of academic fields and industries, this book will be of interest to scholars, researchers, students and policy makers in the fields of security policy, international relations, innovation, European studies and military studies.

Ethical Hacking and Countermeasures: Attack Phases - EC-Council 2009-09-22

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.