Network Defense: Security And Vulnerability Assessment is written by EC-Council in English language. Release on 2010-04-14, this book has 192 page count that enclose valuable information with lovely reading experience. The book was publish by Cengage Learning, it is one of best computers book genre that gave you everything love about reading. You can find Network Defense: Security And Vulnerability Assessment book with ISBN 9781435483590.

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. Proactive vulnerability assessment is key to any organization's security posture. Constant assessment for potential weakness is required to maintain a security edge as new vulnerabilities in operating systems, software, hardware, and even human elements are identified and exploited every day. This book, the fifth in the series, is designed to provide the fundamental knowledge necessary to comprehend overall network security posture and the basic practices in vulnerability assessment. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Network Defense Security And Vulnerability Assessment Related Books

**Network Security Assessment: From Vulnerability to Patch**
This book will take readers from the discovery of vulnerabilities and the creation of the corresponding exploits, through a complete security assessment, all the way through deploying patches against these vulnerabilities to protect their networks. This is unique in that it details both the management and technical skill and tools required to develop an effective vulnerability management system. Business case studies and real world vulnerabilities are used through the book. It starts by introduc...

**Managing A Network Vulnerability Assessment**
The instant access that hackers have to the latest tools and techniques demands that companies become more aggressive in defending the security of their networks. Conducting a network vulnerability assessment, a self-induced hack attack, identifies the network components and faults in policies, and procedures that expose a company to the damage caused by malicious network intruders. Managing a Network Vulnerability Assessment provides a formal framework for finding and eliminating network securi...

**Vulnerability Analysis and Defense for the Internet**
Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or an application. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use. Vulnerability Analysis and Defense for the Internet provides packet captures, flow charts and psuedo code, which enable a user to identify...

**Detection of Intrusions and Malware, and Vulnerability Assessment**
This book constitutes the refereed proceedings of the 8th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2011, held in Amsterdam, the Netherlands, in July 2011. The 11 full papers presented together with two short papers were carefully reviewed and selected from 41initial submissions. The papers are organized in topical sections on network security, attacks, Web security, and host security.

**Guide to Network Defense and Countermeasures**
GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES provides a thorough guide to perimeter defense fundamentals, including intrusion detection and firewalls. This trusted text also covers more advanced topics such as security policies, network address translation (NAT), packet filtering and analysis, proxy servers, virtual private networks (VPN), and network traffic signatures. Thoroughly updated, the new third edition reflects the latest technology, trends, and techniques including virtualization, VMw...

**Penetration Testing and Network Defense**
The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Under...
Hands-On Ethical Hacking and Network Defense

Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and ...

Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach

In this book, the authors adopt a refreshingly new approach to explaining the intricacies of the security and privacy challenge that is particularly well suited to today's cybersecurity challenges. Their use of the threat-vulnerability-countermeasure paradigm combined with extensive real-world examples throughout results in a very effective learning methodology. Charles C. Palmer, IBM Research The Modern Introduction to Computer Security: Understand Threats, Identify Their Causes, and Impl...


PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Fully revised and updated with the latest data from the field, Network Security, Firewalls, and VPNs, Second Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization's network is connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers ...


Related Topics

- Internal Network Vulnerability Assessment
- Network Vulnerability Assessment Report
- Network Vulnerability Assessment Checklist
- Network Vulnerability Assessment Tools
- Network Vulnerability Assessment Definition
- Managing A Network Vulnerability Assessment Blackley
- Managing A Network Vulnerability Assessment Book
- Justin Peltier Managing A Network Vulnerability Assessment
- Guide To Tactical Perimeter Defense Becoming A Security Network Specialist Pdf
- Environmental Vulnerability Assessment Policy Decision Making