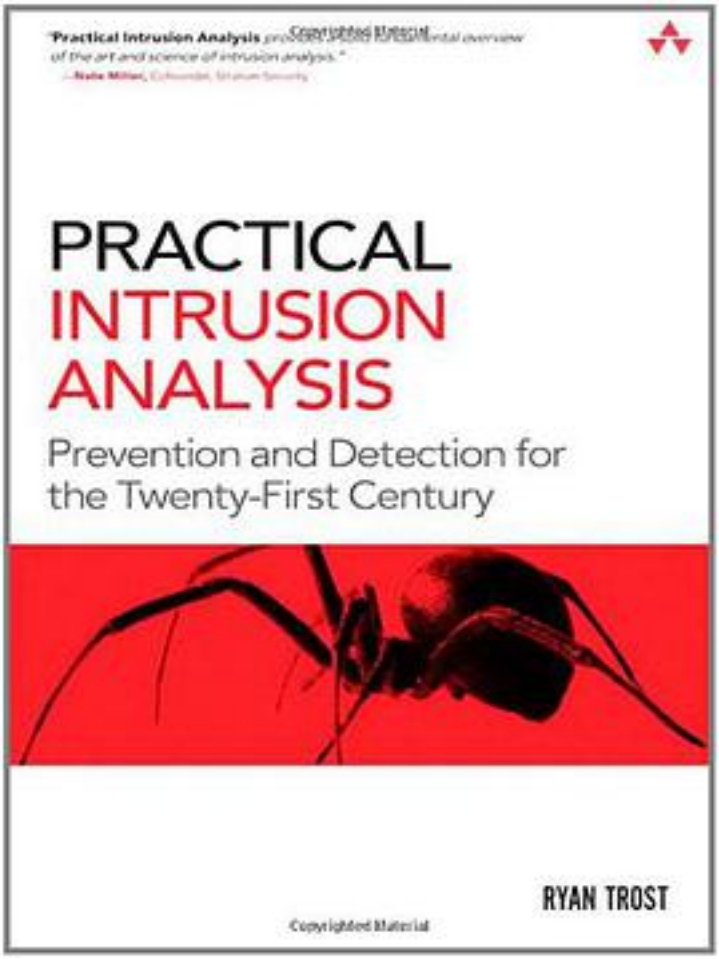
Practical Intrusion Analysis



Practical Intrusion Analysis_下载链接1_

著者:Trost, Ryan

出版者:

出版时间:2009-6

装帧:

isbn:9780321591807

"Practical Intrusion Analysis provides a solid fundamental overview of the art and science of intrusion analysis." -Nate Miller, Cofounder, Stratum Security The Only Definitive Guide to New State-of-the-Art Techniques in Intrusion Detection and

Prevention Recently, powerful innovations in intrusion detection and prevention have evolved in response to emerging threats and changing business environments. However, security practitioners have found little reliable, usable information about these new IDS/IPS technologies. In Practical Intrusion Analysis, one of the field's leading experts brings together these innovations for the first time and demonstrates how they can be used to analyze attacks, mitigate damage, and track attackers. Ryan Trost reviews the fundamental techniques and business drivers of intrusion detection and prevention by analyzing today's new vulnerabilities and attack vectors. Next, he presents complete explanations of powerful new IDS/IPS methodologies based on Network Behavioral Analysis (NBA), data visualization, geospatial analysis, and more. Writing for security practitioners and managers at all experience levels, Trost introduces new solutions for virtually every environment. Coverage includes * Assessing the strengths and limitations of mainstream monitoring tools and IDS technologies* Using Attack Graphs to map paths of network vulnerability and becoming more proactive about preventing intrusions* Analyzing network behavior to immediately detect polymorphic worms, zero-day exploits, and botnet DoS attacks* Understanding the theory, advantages, and disadvantages of the latest Web Application Firewalls* Implementing IDS/IPS systems that protect wireless data traffic* Enhancing your intrusion detection efforts by converging with physical security defenses* Identifying attackers' "geographical fingerprints" and using that information to respond more effectively* Visualizing data traffic to identify suspicious patterns more quickly* Revisiting intrusion detection ROI in light of new threats, compliance risks, and technical alternatives Includes contributions from these leading network security experts: Jeff Forristal, a.k.a. Rain Forest Puppy, senior security professional and creator of libwhisker Seth Fogie, CEO, Airscanner USA; leading-edge mobile security researcher; coauthor of Security Warrior Dr. Sushil Jajodia, Director, Center for Secure Information Systems; founding Editor-in-Chief, Journal of Computer Security Dr. Steven Noel, Associate Director and Senior Research Scientist, Center for Secure Information Systems, George Mason University Alex Kirk, Member, Sourcefire Vulnerability Research Team

作者介绍:

目录:

标签

评论

Practical Intrusion Analysis_下载链接1_

书评

Practical Intrusion Analysis_下载链接1_