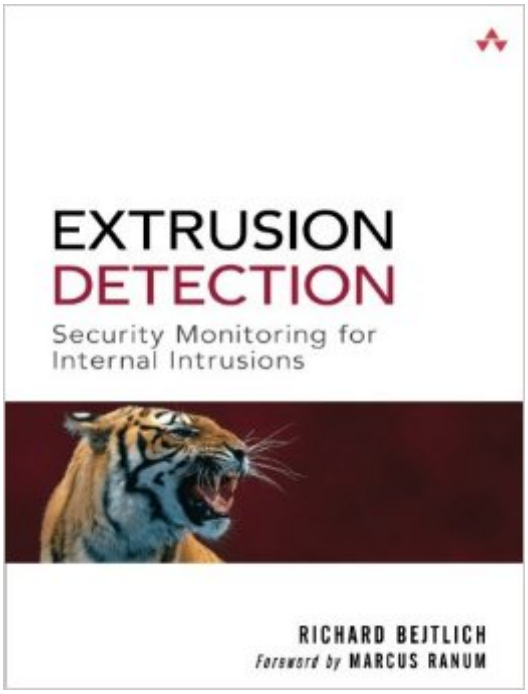
Extrusion Detection: Security Monitoring For Internal Intrusions



Synopsis

Overcome Your Fastest-Growing Security Problem: Internal, Client-Based Attacks Today's most devastating security attacks are launched from within the company, by intruders who have compromised your users' Web browsers, e-mail and chat clients, and other Internet-connected software. Hardening your network perimeter won't solve this problem. You must systematically protect client software and monitor the traffic it generates. Extrusion Detection is a comprehensive guide to preventing, detecting, and mitigating security breaches from the inside out. Top security consultant Richard Bejtlich offers clear, easy-to-understand explanations of today's client-based threats and effective, step-by-step solutions, demonstrated against real traffic and data. You will learn how to assess threats from internal clients, instrument networks to detect anomalies in outgoing traffic, architect networks to resist internal attacks, and respond effectively when attacks occur. Bejtlich's The Tao of Network Security Monitoring earned acclaim as the definitive guide to overcoming external threats. Now, in Extrusion Detection , he brings the same level of insight to defending against today's rapidly emerging internal threats. Whether you're an architect, analyst, engineer, administrator, or IT manager, you face a new generation of security risks. Get this book and protect yourself. Coverage includes Architecting defensible networks with pervasive awareness: theory, techniques, and tools Defending against malicious sites, Internet Explorer exploitations, bots, Trojans, worms, and more Dissecting session and full-content data to reveal unauthorized activity Implementing effective Layer 3 network access control Responding to internal attacks, including step-by-step network forensics Assessing your network's current ability to resist internal attacks Setting reasonable corporate access policies Detailed case studies, including the discovery of internal and IRC-based bot nets Advanced extrusion detection: from data collection to host and vulnerability enumeration About the Web Site Get book updates and network security news at Richard Bejtlich's popular blog, taosecurity.blogspot.com, and his Web site, www.bejtlich.net.

Book Information

Paperback: 416 pages
Publisher: Addison-Wesley Professional (November 18, 2005)
Language: English
ISBN-10: 0321349962
ISBN-13: 978-0321349965
Product Dimensions: 6.9 x 1 x 9 inches

Shipping Weight: 1.6 pounds (View shipping rates and policies)
Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (12 customer reviews)
Best Sellers Rank: #1,053,889 in Books (See Top 100 in Books) #140 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Computer Design #252 inÂ Books > Computers & Technology > Certification > CompTIA #496 inÂ Books > Computers & Technology > Hardware & DIY > Design & Architecture

Customer Reviews

Following the success of 'The Tao of Network Security Monitoring' last year, world renowned security expert Richard Bejtlich raises once again the standard for security professionals, this time by focusing on analyzing threats coming from within our network - a kind of underestimated area.Traditionally, the point of network security is about keeping the bad guys out of a network Â¡V Â¡Ã Â¥outÂ¡Ã Â¦ being where we hope they are to start with. Possible points of entry are considered to be devices accessible from the outside in some way, mostly servers and perhaps routers. Workstations with no address on the network have no apparent footprint that would betray their existence, so if potential intruders don't even know the hosts exist, and are unable to make any connection to them, how could they possibly exploit them? The truth is they can, in many ways, using not only technical skills but imagination and ability to exploit the human factor - against which no automated procedure or device can defend for long.Furthermore, many administrators put all their effort and resources into trying to design an impenetrable network infrastructure, but ignore the fact that every prevention measure is bound to fail at any moment. These administrators put little or no thought into the possibility of a real intrusion and, as a result, when it occurs the network infrastructure they've built doesn't allow them to cut their losses to a minimum, regain control in a timely manner and collect credible evidence that may lead to a future investigation.This, Richard Bejtlich's second book on the subject of network security, attempts to establish into readers' minds a solid grounding on how things are, while emphasizing common misconceptions of the past.

First, this book should be called The Engineers Guide to Implementing Security to Detect and Prevent Malicious Traffic in Your Network. This is a very thorough book on how to detect malicious traffic leaving a network (hence Extrusion), with great illustrations and walkthroughs. There are chapters on planning, deployment, tuning and other key, often overlooked, aspects surrounding the wonderful world of Intrusion Detection.The first hint that this book was a bit different is noticed in the Foreward. Marcus Ranum wrote the forward, or I should say guided the direction of the Foreward.

Marcus opts for an interview with the author, versus "telling you a bunch of stuff about the book". The Foreward is a must when browsing this book. Very creative, something perhaps missing in the world of Information Security these days.After the foreward, chapters include Defensible Network Architecture, a brief overview of IDS, Enterprise network Instrumentation (packet captures, tools and some techniques), Layer 3 Network Access Control, Traffic Threat Assessment, Network Incident Response, Network Forensics, and Internal Intrusions that discuss Traffic Threat Assessment Case Study and Malicious Bots. There are several Appendixes as well (a requirement for all technical books) that include how to Collect Session Data, minimal Snort Installation Guide, Enumeration Methods (identifying systems on a network), and Open Source Host Enumeration (doing it for free).The author uses firewall technology, proxy technology, and IDS technology to define how to monitor and control traffic entering or leaving a network. Specific configurations that could be copied line by line and implemented into a network are provided.Richard leaves nothing to the imagination in this book.

Now, they say that one way to be happy is to have low expectations about stuff. In case of me and this book, the opposite has happened: my expectations were really high. In fact, I was counting days until the book's arrival. Do not get me wrong, it's an excellent book, but it seems to fall slightly short of my lofty expectations.My first unmet expectation was the term `extrusion' itself. I suspected that the book will have more coverage of real insider attacks, and not just infected misbehaving client PCs. The author does say that some use the term `extrusion' to refer to intellectual property theft (or `IP leakage') in his section on the `History of Extrusion Detection', but does not follow up on that. His definition of `extrusion detection' seem to be closer to the `detection of consequences of intrusion in the form of outbound connections', such as after a client-targeting attack, rather than a separate phenomenon of a trusted insider attack.The second thing I did not quite like was too much overlapping material with Richard's previous book, `Tao of Network Security Monitoring.' For example, security process and security principles sections seem to be taken from his Tao book (which is a superb book, by itself!). Similarly, in my opinion, an in depth coverage of NSM methodology and `network forensics', presented in the Tao book should not have been repeated since the differences between applying NSM for intrusion and extrusion detection are really minor.And, I liked pretty much everything else: detailed examples of `traffic threat assessment', unmatched technical accuracy, easy to follow style, etc. Coverage of bots in chapter 10 deserves a favorable mention as well as a strategy for network incident response.

Extrusion Detection: Security Monitoring for Internal Intrusions The Practice of Network Security Monitoring: Understanding Incident Detection and Response Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network) Fetal Heart Monitoring: Principles and Practices (AWHONN, Fetal Heart Monitoring) Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC-Council Press) Understanding Extrusion 2E Extrusion, Second Edition: The Definitive Processing Guide and Handbook (Plastics Design Library) Hot-Melt Extrusion: Pharmaceutical Applications Social Security: Time for a Life of Leisure - The Guide of Secrets to Maximising Social Security Retirement Benefits and Planning Your Retirement (social ... disability, social security made simple) Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan Grenada And Soviet/cuban Policy: Internal Crisis And U.s./oecs Intervention (Westview Special Studies in National Security and Defense Policy) Practical Machine Learning: A New Look at Anomaly Detection Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection (Data-Centric Systems and Applications) Linux Firewalls: Attack Detection and Response Detection and Estimation for Communication and Radar Systems How to get Rid of Lice - All About Lice : Lice Treatment,Detection,Management Sun Sense: A Complete Guide to Prevention, Early Detection and Treatment of Skin Cancer Emerging Issues of Credit Card Frauds and their Detection Techniques using Genetic Algorithm Optimal Fault Detection and Resolution During Maneuvaring for AutonomousUnderwater Vehicles