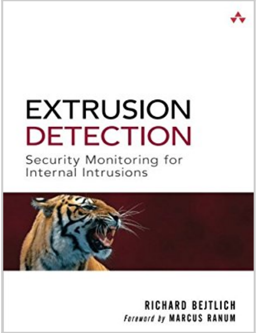

Extrusion Detection: Security Monitoring for Internal Intrusions

By Richard Bejtlich

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich

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.

Extrusion Detection: Security Monitoring for Internal Intrusions

By Richard Bejtlich

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich

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.

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich Bibliography

- Rank: #739283 in Books
- Published on: 2005-11-18
- Released on: 2005-11-08
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.00" w x 6.90" l, 1.49 pounds
- Binding: Paperback
- 416 pages

Editorial Review

From the Back Cover

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 includesArchitecting defensible networks with pervasive awareness: theory, techniques, and tools Defending against malicious sites, Internet Explorer exploitations, bots, Trojans, worms, and moreDissecting session and full-content data to reveal unauthorized activityImplementing effective Layer 3 network access controlResponding to internal attacks, including step-by-step network forensics Assessing your network's current ability to resist internal attacksSetting reasonable corporate access policiesDetailed case studies, including the discovery of internal and IRC-based bot netsAdvanced 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.

About the Author

Richard Bejtlich is founder of TaoSecurity, a company that helps clients detect, contain, and remediate intrusions using Network Security Monitoring (NSM) principles. He was formerly a principal consultant at Foundstone--performing incident response, emergency NSM, and security research and training--and created NSM operations for ManTech International Corporation and Ball Aerospace & Technologies Corporation. For three years, Bejtlich defended U.S. information assets as a captain in the Air Force Computer Emergency Response Team (AFCERT). Formally trained as an intelligence officer, he is a graduate of Harvard University and of the U.S. Air Force Academy. He has authored or coauthored several security books, including *The Tao of Network Security Monitoring* (Addison-Wesley, 2004).

Welcome to *Extrusion Detection: Security Monitoring for Internal Intrusions.* The goal of this book is to help you detect, contain, and remediate internal intrusions using network security monitoring (NSM) principles. This book will guide security architects and engineers who control and instrument networks, help analysts and operators to investigate internal network security events, and give technical managers the justification they need to fund internal security projects. *Extrusion Detection* is the sequel to my first book, *The Tao of Network Security Monitoring: Beyond Intrusion Detection.* While *Extrusion Detection* is a stand-alone work, I strongly recommend reading *The Tao* first, or at least having it nearby as a reference.

Those of you who have read *The Tao* will recall that the book focused on outsiders gaining unauthorized access to Internet-exposed servers. This threat model reflected the predominant mode of Internet exploitation in the 1990s. The primary means for attackers to exploit targets during the 1990s involved server-side attacks. Intruders gained unauthorized access by exploiting services offered by Internet-facing victims. Typical targets included Web servers, e-mail servers, domain name resolution (DNS) servers, and other programs that wait to answer queries from Internet users. [1] If internal workstations were not obscured by network address translation (NAT) gateways or firewalls, they too could be attacked directly, but only if they offered services similar to the typical targets. Local file-sharing services employing Unix remote procedure calls (RPCs) or Windows Server Message Block (SMB) were high-priority targets.

With the advent of the firewall in the early 1990s and the adoption of private Request for Comments (RFC) 1918 space in the middle 1990s, internal workstations were seldom directly attacked, unlike their public server counterparts. Protection from the outsider threat required access control and limits on the exposure of Internet-facing hosts. Traditional monitoring efforts watched attacks from the Internet to exposed servers because intruders most often launched "server-side" attacks.

The current decade has seen this model turned inside-out. Beginning in 2000, and with increasing intensity since 2003, corporate and home users have been subjected to increasing numbers of "client-side" attacks. No longer are services offered by computers the only targets of attack. Now, the applications upon which users rely, such as Web browsers, e-mail clients, and chat programs are the targets.

Instead of an intruder attacking the Web server running on a company's Internet-facing server, the intruder attacks the Web browser of an internal user who surfs intentionally or accidentally to a malicious Web site. Alternatively, a user may receive a Trojan through a chat program and unwisely decide to run that executable while operating with administrator privileges. No longer is it sufficient for security staff to harden the network perimeter by limiting services exposed to the Internet. The perimeter network is still a crucial part of network infrastructure, despite calls for the "de-perimeterization" of enterprise networks. Now, software running on clients must be protected, and the traffic generated must be monitored for signs of compromise.

This book focuses on ways to deal with the threat to internal systems. By "internal systems," I mean those considered to be intranet, not Internet, hosts. Extrusion Detection is not about traditional hardening of internal hosts to the same degree as external hosts. Traditional internal host hardening means minimizing services offered by systems, thereby decreasing the likelihood of server-side attacks. In other words, I would not be offering new advice if I discussed how to control and detect attacks against the SMB server running on port 445 TCP on a Windows XP workstation. I may not address such practices in detail here, but reduction of server-side exposure is certainly a beneficial security practice.

Extrusion Detection explains how to engineer an internal network that can control and detect intruders launching server-side or client-side attacks. Client-side attacks are more insidious than server-side attacks, because the intruder targets a vulnerable application anywhere inside a potentially hardened internal network. A powerful means to detect the compromise of internal systems is to watch for outbound connections from the victim to systems on the Internet operated by the intruder. Here we see the significance of the word "extrusion" in the book's title. That is, in addition to watching connections inbound from the Internet, we watch for suspicious activity exiting the protected network.

Audience

This book is for architects, engineers, analysts, operators, and managers with intermediate to advanced knowledge of network security. Architects will learn ways to design networks better suited to surviving client-side (and server-side) attacks. Primarily using open source software, engineers will learn how to build solutions for controlling and instrumenting internal networks. Analysts and operators will learn how to interpret the data collected in order to discover and escalate indicators of compromise. Managers will read case studies of real malicious software and the consequences of poor internal security.

All readers will learn about the theory, techniques, and tools for implementing network security monitoring (NSM) for internal intrusions. Executives may use the material to assess the state of their networks in relation to the book's recommended best practices. Auditors can determine if their clients are collecting the network-based information that's needed for the appropriate control, detection, and response to intrusions.

Prerequisites

I have attempted to avoid duplication of material presented in other books, including *The Tao.* My purpose here is to publish as much new thought on internal security as possible and to have this book be a complement to previously published books. I expect my audience to bring a certain amount of knowledge to the table.

Core skills readers should possess in order to get the most from the book are:

- Scripting and Programming: Familiarity with simple shell scripting is helpful when automating certain tasks.
- Weapons and Tactics: Knowledge of tools and techniques for network attack and defense is assumed.
- System Administration: Readers should be comfortable with installing software on the operating systems they use.
- Telecommunications: An understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) networking is absolutely essential.
- Management and Policy: Appreciation of the laws, regulations, and other restrictions associated with network security is highly recommended.

Readers who believe they may be lacking in any of these areas can benefit from my recommended reading list, which is constantly updated and available at http://www.bejtlich.net/reading.html.

If I were to recommend a single book to read prior to this one, it would be The *Tao of Network Security Monitoring: Beyond Intrusion Detection.* In many ways, *Extrusion Detection* is an attempt to extend *The Tao* to the addressing of internal threats. While *Extrusion Detection* will function as a stand-alone work, your network security monitoring operations will greatly benefit from your reading *The Tao.*

A Note on Operating Systems

Where possible, the reference platform for this book is FreeBSD 5.3 or 5.4 RELEASE. In the cases where Linux is required, I use Slackware Linux 10.0. Some of the latest innovations in host-centric access control are supported only on commercial operating systems such as Microsoft Windows.

Generally speaking, any tool that compiles on FreeBSD will work on the Unix variant you choose. Tools that are closely tied to the OS kernel, such as the Packet Filter (Pf) firewall (http://www.openbsd.org/faq/pf/), may not be available on any OS other than those specified later in the book.

Scope

Extrusion Detection is divided into three parts that are followed by an epilogue and appendices. You can focus on the areas that interest you, because the sections are modular. You may wonder why greater attention is not paid to popular tools like Nmap or Snort. With *Extrusion Detection*, I hope to continue breaking new ground by highlighting ideas and tools seldom seen elsewhere. If I don't address a widely popular product, it's because it has received plenty of coverage in another book.

Part I mixes theory with architectural considerations. Chapter 1 is a recap of the major theories, tools, and techniques from *The Tao*. It is important for readers to understand that NSM has a specific technical meaning and that NSM is not the same process as intrusion detection or prevention. Chapter 2 describes the architectural requirements for designing a network best suited to detect, control, and respond to intrusions. Chapter 3 explains the theory of extrusion detection and sets the stage for the remainder of the book. Chapter 4 describes how to gain visibility to internal traffic. Part I concludes with Chapter 5, original material by financial security architect Ken Meyers that explains how internal network design can enhance the control and detection of internal threats.

Part II is aimed at security analysts and operators; it is traffic-oriented and requires basic understanding of TCP/IP and packet analysis. Chapter 6 offers a method of dissecting session and full content data to unearth unauthorized activity. From a network-centric perspective, Chapter 7 offers guidance on responding to intrusions. Chapter 8 concludes Part II by demonstrating principles of network forensics. The last two chapters are unique in that they use the term "network" to not mean "computer" or "enterprise." When I talk about network incident response or network forensics, I refer to traffic-oriented techniques and tools. This approach stands in sharp contrast to the host-centric methodologies found elsewhere. My material complements and does not replace those valuable resources.

Part III collects case studies of interest to all types of security professionals. Chapter 9 applies the lessons of Chapter 6 and explains how an internal bot net was discovered using traffic threat assessment. Chapter 10 exposes the inner workings of bot nets, through the eyes of Mike Heiser. As an analyst at Myrtle Beach-based managed security service provider LURHQ, Michael has a unique perspective that readers will appreciate.

An epilogue points to future developments. Appendix A describes how to install Argus and NetFlow collection tools to capture session data. Appendix B explains how to install a minimal Snort deployment in an emergency. Appendix C, by Tenable Network Security founder Ron Gula, examines the variety of host and vulnerability enumeration techniques available in commercial and open source tools. The book concludes with Appendix D, where Red Cliff Consulting expert Rohyt Belani offers guidance on internal host enumeration using open source tools.

Subjects Beyond the Scope of This Book

I do not address the following topics in this book, consistent with my desire to avoid repeating material best addressed elsewhere (if possible). If you want to know more about these subjects, you may find the following books helpful.

- Viruses, worms, and malware. *The Art of Computer Virus Research and Defense* by Peter Szor (Upper Saddle River, NJ: Addison-Wesley, 2005); *Malware: Fighting Malicious Code* by Ed Skoudis and Lenny

Zeltser (Upper Saddle River, NJ: Prentice Hall, 2004).
- Phishing. *Phishing: Cutting the Identity Theft* Line by Rachael Lininger (Boston, MA: John Wiley & Sons, 2005) or *Phishing Exposed* by Lance James (Boston, MA: Syngress, 2006).
- Spam. *Anti-Spam Toolkit* by Paul Wolfe, Charlie Scott, and Mike W. Erwin (New York, NY: McGraw-Hill/Osborne, 2004); *Inside the Spam Cartel by Spammer-X* (Rockland, MA: Syngress, 2004); *Slamming Spam: A Guide for System Administrators* by Robert Haskins and Dale Nielsen (Upper Saddle River, NJ: Addison-Wesley, 2005).
- Denial of Service. *Internet Denial of Service: Attack and Defense Mechanisms* by Jelena Mirkovic, et al. (Upper Saddle River, NJ: Prentice Hall, 2005).

Book Web Site

For more information on network security monitoring and extrusion detection, visit http://www.extrusiondetection.com.

[1] In mid-August 2005, the Zotob worm is winding its way across the Internet by attacking SMB services on vulnerable Windows workstations. Even in late 2005, the traditional server-side attack is alive and well, alongside more recent client-side attacks. More information on Zotob is available at http://www.f-secure.com/v-descs/zotob_a.shtml.

0321349962P10262005

Users Review

From reader reviews:

Bertha Morrison:

As people who live in the particular modest era should be up-date about what going on or data even knowledge to make these people keep up with the era that is always change and make progress. Some of you maybe may update themselves by reading through books. It is a good choice for you personally but the problems coming to you is you don't know which you should start with. This Extrusion Detection: Security Monitoring for Internal Intrusions is our recommendation to make you keep up with the world. Why, because book serves what you want and want in this era.

William Kelley:

Now a day individuals who Living in the era wherever everything reachable by talk with the internet and the resources included can be true or not call for people to be aware of each data they get. How many people to be smart in receiving any information nowadays? Of course the answer is reading a book. Reading through a book can help folks out of this uncertainty Information especially this Extrusion Detection: Security Monitoring for Internal Intrusions book since this book offers you rich data and knowledge. Of course the knowledge in this book hundred percent guarantees there is no doubt in it as you know.

Miranda Durkee:

You can find this Extrusion Detection: Security Monitoring for Internal Intrusions by browse the bookstore or Mall. Simply viewing or reviewing it may to be your solve challenge if you get difficulties for ones knowledge. Kinds of this reserve are various. Not only simply by written or printed but additionally can you enjoy this book by means of e-book. In the modern era like now, you just looking by your local mobile phone and searching what their problem. Right now, choose your own ways to get more information about your publication. It is most important to arrange yourself to make your knowledge are still upgrade. Let's try to choose suitable ways for you.

Elizabeth Sherer:

As a student exactly feel bored for you to reading. If their teacher asked them to go to the library or make summary for some book, they are complained. Just little students that has reading's soul or real their hobby. They just do what the educator want, like asked to go to the library. They go to right now there but nothing reading critically. Any students feel that studying is not important, boring as well as can't see colorful images on there. Yeah, it is to be complicated. Book is very important for you personally. As we know that on this period, many ways to get whatever you want. Likewise word says, many ways to reach Chinese's country. So , this Extrusion Detection: Security Monitoring for Internal Intrusions can make you experience more interested to read.

Download and Read Online Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich #BOJ6F5VQPKC

Read Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich for online ebook

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich books to read online.

Online Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich ebook PDF download

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich Doc

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich Mobipocket

Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich EPub

BOJ6F5VQPKC: Extrusion Detection: Security Monitoring for Internal Intrusions By Richard Bejtlich