《网络安全监控实战》

图书基本信息

书名：《网络安全监控实战》

13位ISBN编号：9787111498658

出版时间：2015-4

作者：Richard Bejtlich

译者：蒋蓓,姚领田,李潇,张建

《网络安全监控实战》

作者简介

理查德·贝特利奇(Richard Bejtlich)现任全球顶级安全公司FireEye的首席安全战略官、美国前沿网络安全公司Mandiant的首席安全官，曾任通用电气事件响应的主管，是最早一批研究网络安全和NSM防御的践行者。他毕业于哈弗大学和美国空军学院，著有《The Tao of Network Security Monitoring》、《Extrusion Detection》和《Real Digital Forensics》。
他还在博客和推特上创作，其博客地址为http://taosecurity.blogspot.com；推特账号为@taosecurity。

《网络安全监控实战》

精彩短评

1、见 The Practice of Network Security Monitoring 书评
2、本书主要讲了网络安全监控的主要原理，采用检测和响应的网络监控思想，在网络中部署NSM，对网络流量和数据进行收集、分析和预警。本书以SO作为NSM实践的工作，讲解了SO的部署，以及SO相关工具，包括Tcpdump，wireshark，networkminer等的具体实用方法，在NSM实践中的操作流程，如何监控服务器/客户端的网络检测和响应的具体案例。本书网络安全监控内容比较细致，工具的可操作性强，是一本网络安全的入门好书。
3、今年读的最好的技术书籍，专业的译者，翻译非常易读。迄今为止国内安全类别翻译书籍里面的用心之作。
4、这本书看似重点讲了网络监控的工具和应用，但实际上在操作过程中则体现了当前安全趋势---由防御到检测和响应的转变。而检测和响应的关键是数据分析。本书内则是通过实践来娓娓道来分析和取证。
对于客户端监控和分析的章节，也间接地介绍了对内网的持续渗透方法和思路：）

对了，书中好多地方以apt1为例来说明。不了解的可以看下这个报告.....完全针对我军的嘛

5、关于网络安全监控理论方面的内容偏少，方法论也不多，大量的篇幅在介绍SO的安装部署与使用，属于工具说明书。

《网络安全监控实战》

精彩书评

1、我们知道安全组件阻塞威胁firewall阻塞IPS阻塞anti-AV阻塞DLP阻塞DRM阻塞（这个国内刚起步）而好的网络安全监控，需要以威胁识别为核心，数据分析为驱动的将这些安全组件联通起来。说到数据驱动，当然要应用数据分析的技巧，包括如何搜集数据（包括在哪里放置哪些数据产生工具），如何分析数据（检测），如何展示分析结果（响应）。其中第一步知道搜集哪些数据是非常重要的：这本书告诉了我们建议收集的数据类型(1) Full Content Dataall information that passes across a network. We aren’t filtering the data to collectonly information associated with security alerts. We’re not saving applicationlogs. We’re making exact copies of the traffic as seen on the wire(2) extracted content datarefers to high-level data streams—such as files, images, and media—transferred between computers. Unlike with full content data, which includes headers from lower levels of the communication process,with extracted content, we don’t worry about MAC addresses, IP addresses,IP protocols, and so on. Instead, if two computers exchange a file, we reviewthe file. If a web server transfers a web page to a browser, we review the webpage. And, if an intruder transmits a piece of malware or a worm, we reviewthe malware or worm.(2) session Dataa record of the conversation between two network nodes. AnNSM tool like Bro (http://www.bro.org/) can generate many types of logsbased on its inspection of network traffic.(3) transaction dataTransaction data is similar to session data, except that it focuses on understanding the requests and replies exchanged between two network devices.(4) statistical datadescribes the traffic resulting from various aspects of an activity.(5) metadata(6) alert dataAlert data reflects whether traffic triggers an alert in an NSM tool. Anintrusion detection system (IDS) is one source of alert data.

《网络安全监控实战》

版权说明