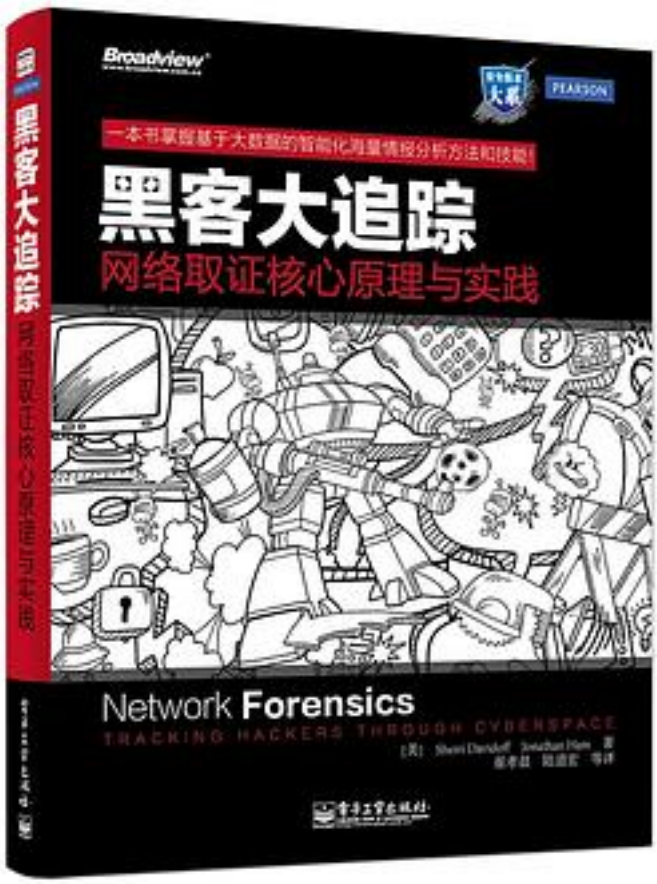
黑客大追踪



黑客大追踪_下载链接1_

著者:[美] Sherri Davidoff

出版者:电子工业出版社

出版时间:2015-1

装帧:平装

isbn:9787121245541

网络取证是计算机取证技术的一个新的发展方向，是计算机网络技术与法学的交叉学科。《黑客大追踪：网络取证核心原理与实践》是网络取证方面的第一本专著，一经出版便好评如潮，在Amazon网站上的评分达4.5星。

《黑客大追踪：网络取证核心原理与实践》根据网络取证调查人员的实际需要，概述了网络取证的各个方面，不论是对各种网络协议的分析和对各种网络设备的处理方式，还是取证流程的设计都有独到之处。

《黑客大追踪：网络取证核心原理与实践》共分四大部分十二章，第1章“实用调查策略”，第2章“技术基础”和第3章“证据获取”属于第一部分，其中给出了一个取证的方法框架，并介绍了相关的基础知识；第4章“数据包分析”，第5章“流统计分析”、第6章“无线：无须网线的取证”和第7章“网络入侵的侦测及分析”属于第二部分，介绍了对网络流量进行分析的各种技术；第8章“事件日志的聚合、关联和分析”、第9章“交换器、路由器、防火墙”和第10章“Web代理”属于第三部分，详述了在各种网络设备和服务器中获取和分析证据的方法。第11章“网络隧道”和第12章“恶意软件取证”属于第四部分，针对网络隧道和恶意软件分析这两个网络取证中的难点和热点问题展开讨论。

《黑客大追踪：网络取证核心原理与实践》在学术理论上具有交叉性、前沿性和创新性，在实践应用中注重可操作性和实用性。可作为网络安全/计算机取证专业的教材，对于司法工作者、律师、司法鉴定人和IT从业人员，也具有良好的参考价值。

作者介绍:

目录: 第一部分 基础篇

・・・・・・・(收起)

黑客大追踪_下载链接1_

标签

安全

网络

取证

计算机

网络战

网络取证

黑客大追踪

美国

评论

2016-11：1作为教材来用，对技术和操作层面介绍较多，但理论方面较少。实践方面，对新手的引导例子较少。许多分析的数据集若能提供作为训练会更好。

全是优点，但是很简洁了

毫无实用价值 专程来刷恶评的！~~

挺好的一本书。对网络取证的场景和维度覆盖的还算全，方法论和思路不错的。算是事件和理论并重。 尤其是在有幸参加了Sherri的取证课程后，更是觉得不错

工作需要 找来翻了翻 书中用到wireshark等软件的地方好多……

讲的太皮毛了，本打算用来开拓思维的。

我能说这本书拉低了安全技术大系的水准么，翻译也是一般

黑客大追踪_下载链接1_

书评

黑客大追踪_下载链接1_