

<<应急响应&计算机司法鉴定>>

图书基本信息

书名：<<应急响应&计算机司法鉴定>>

13位ISBN编号：9787302097273

10位ISBN编号：7302097275

出版时间：2004-11-1

出版时间：清华大学出版社

作者：汪青青, Kevin Mandia, Chris Prosise, Matt Pepe, 付宇光

页数：400

字数：594000

译者：汪青青, 付宇光

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<应急响应&计算机司法鉴定>>

### 内容概要

周边安全技术的有效性和分析能力正在提高。

计算机司法鉴定技术也同样如此。

但是，未知因素是管理和分析计算机数据的人。

不管是执法官员、私人调查员、信息安全专家、顾问，或者是其他安全专家，成功防止和响应网络威胁的关键在于对计算机证据的合理鉴定、收集、保存和分析。

本书提供了有效响应突发事件、收集计算机司法鉴定证据和分析合适的日志、文件所必需的知识、技巧和工具。

这同时提高了各单位对突发事件的处理能力，或者事发前就汲取了教训。

一盎司的预防效果等于一磅的治疗。

另外，本书还介绍了如何获取可能留下痕迹的位置和可能的对调查目标的警告，从而可以帮助公司或司法部门调查员主动执行在线调查。

现在，公司的宝贵资料通常放在计算机中，这容易受到知识渊博的内部人员或机智的计算机黑客的攻击，他们可能敲诈你、贩卖信息，或将信息公布到Internet。

当然，如果需要处理敏感问题，那么在采取措施之前，应该咨询安全部门、律师、知识丰富的计算机司法鉴定咨询公司(最好有执法或情报方面的经验)或执法机构。

总而言之，每个信息安全专家——不管是系统管理员、调查员、顾问或者执法官员——都应该遵循本书的建议。

信息系统内忧外患，受过良好训练的协同保护、应急响应和司法鉴定分析团队对于所有要保护自身和财产免受网络威胁的组织而言，都是必需的。

## <<应急响应&计算机司法鉴定>>

### 作者简介

Kevin Mandia是Foundston公司的计算机司法鉴定部门的主管。他领导计算机司法鉴定专业小组，在过去的一年中，着手处理了在电子商务和金融服务单位发生的超过30起的计算机安全事故。他还协助美国空军、美国联邦调查局和其他执法部门来处理一些正在调查的案子。

## &lt;&lt;应急响应&amp;计算机司法鉴定&gt;&gt;

## 书籍目录

第1部分 简介 第1章 现实生活中的突发事件 1.1 影响响应的因素 1.2 跨国犯罪 1.3 传统的黑客行为 1.4 小结 第2章 应急响应过程简介 2.1 计算机安全事件的意义 2.2 应急响应的目标 2.3 应急响应小组参与人员 2.4 应急响应方法 2.5 小结 2.6 问题 第3章 为应急响应做准备 3.1 突发事件预防准备概述 3.2 识别风险 3.3 单个主机的准备工作 3.4 准备网络 3.5 制订恰当的策略和规程 3.6 创建响应工具包 3.7 建立应急响应小组 3.8 小结 3.9 问题 第4章 应急响应 4.1 初始响应阶段概述 4.2 建立突发事件通知程序 4.3 记录事发详情 4.4 突发事件声明 4.5 组建CSIRT 4.6 执行例行调查步骤 4.7 约见 4.9 小结 4.10 问题

第2部分 数据收集 第5章 Windows系统下的现场数据收集 5.1 创建响应工具箱 5.2 保存初始响应信息 5.3 获取易失性数据 5.4 进行深入的现场响应 5.5 制作司法鉴定复件的必要性 5.6 小结 5.7 问题 第6章 Unix系统下的现场数据收集 6.1 创建响应工具包 6.2 保存初始响应信息 6.3 在进行司法鉴定复制之前获得易失性数据 6.4 进行深入的现场响应 6.5 小结 6.6 问题 第7章 司法鉴定复件 7.1 可作为呈堂作证的司法鉴定复件 7.2 司法鉴定复制工具的要求 7.3 制作硬盘的司法鉴定复件 7.4 制作合格的司法鉴定硬盘复件 7.5 小结 7.6 问题 第8章 收集网络证据 8.1 网络证据 8.2 网络监视的目的 8.3 网络监视的类型 8.4 安装网络监视系统 8.5 执行陷阱跟踪 8.6 用tcpdump进行全内容监视 8.7 收集网络日志文件 8.8 小结 8.9 问题 第9章 证据处理 9.1 证据 9.2 证据处理 9.3 证据处理程序概述 9.4 小结 9.5 问题

第3部分 数据分析 第10章 计算机系统存储基础 10.1 硬盘与接口 10.2 准备硬盘 10.3 文件系统和存储层介绍 10.4 小结 10.5 问题 第11章 数据分析技术 11.1 司法鉴定分析的准备工作 11.2 恢复司法鉴定复件 11.3 在Linux下准备分析用的司法鉴定复件 11.4 用司法鉴定套件检查映像文件 11.5 将合格的司法鉴定复件转换成司法鉴定复件 11.6 在Windows系统中恢复被删除的文件 11.7 恢复未分配空间、自由空间和松弛空间 11.8 生成文件列表 11.9 准备用于查找字符串的驱动器 11.10 小结 11.11 问题 第12章 调查Windows系统 第13章 调查Unix系统 第14章 网络通信分析 第15章 黑客工具研究 第16章 研究路由器 第17章 撰写计算机司法鉴定报告

第4部分 附录 附录A 问题解答 附录B 应急响应表格

<<应急响应&计算机司法鉴定>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>