<<Windows取证分析>>

图书基本信息

书名：<<Windows取证分析>>

13位ISBN编号：9787030233080

10位ISBN编号：7030233085

出版时间：2009-1

出版时间：科学出版社

作者：HarlanCarvey

页数：222

字数：320000

前言

自从1991年在美国召开的国际计算机专家会议上首次提出“计算机取证（Corn-puter Forensic）”术语以来，随着互联网的普及和计算机犯罪案件的增多，计算机取证一直是信息安全领域中的热门话题，国际上几乎每年都要召开以计算机取证为主题的学术会议，用于计算机取证的技术工具逐渐发展成为信息安全产业的一个特殊种类，甚至很快也有了诸如“国际计算机证据组织（IOCE）”之类的“非政府”组织。

自然，近年有关计算机取证的专业书籍也出版不少，其中涉及基础理论、取证技术和取证工具的专著先后被译介到国内，这些工作对国内计算机取证的研究和实践都起到了十分重要的推动作用。

因而，当王智慧先生将他与几位朋友的译著《Windows取证分析》的清样送来之后，我是怀着几分欣喜，利用两个周末的余暇认真奉读的。

所以如此，一是因为智慧本人一直致力于，也乐于、长于计算机取证工作，在理论功底和实践经验上颇有见地并屡建奇功，能人他法眼的书籍自有不凡之处；二是因为对Windows的取证是现实生活中最常见，也最复杂的一项工作。

据智慧介绍，原书作者Harlan Carvey曾在美国军方长期从事信息安全工作，有过十多年的取证工作经验，并且有过《Windows取证和事件恢复》一书面世，颇受业内人士推崇。

有着这样的专业背景，加上今年岁末难得的晴天暖阳，我的两个周末是在愉快地阅读中度过的。

掩卷之时，正值满月初升。

回味本书，觉得有三点特别的感受不得不说：一是知识内容上的创新。

初看书名，很容易会先人为主地把它看作作者旧作《Windows取证和事件恢复》的翻版。

其实不然，正如作者在前言中声明的，他不想将此书写成旧作的续集，细读本书中对开机取证、注册表分析的深入解析和在文件分析、内存分析、Root-kits分析方面的独到体会，你会相信作者说到做到了。

二是技术工具上的创意。

本书介绍了不少现实可用的取证工具，这些工具能帮助读者更好地理解和体会作者在书中提出和阐述的概念，而且这些工具并非对Encase之类的商业产品的简单罗列，而是精选了不少当下热门的“活的”网上新宠，尤其可喜的是，有的工具就是作者本人的杰作，用自己的看家本领说事，应该算是有创意。

三是实践经验上的创见。

由于作者在此领域有十多年的工作经验，本书中列举的实例很多是自身实践的积累，不少实例是在其他同类书籍中找不到的。

例如结合英国布莱尔政府Word格式文档的信息泄露案例，作者介绍的与“对象链接嵌入技术（OLE）流”相关的信息痕迹与恢复经验，以及反复强调的可重复性和取证数据的自动化处理等体会，也都是其他著述鲜有涉猎的。

当然，如果要说本书不够过瘾的地方，可能要算第6章“可执行文件分析”部分，这本是当前恶意软件（间谍软件）作恶的重要环节。

由于涉及逆向工程技术，作者的意见是可以就此另写一本书，因而分析不深。

另外，从理论上讲，本书对分布式取证、自动化取证的后处理、数据挖掘和包括交换文件、休眠文件等在内的内存分析等热点问题尚可再深入一些。

考虑到本书专为实践需要而写，面面俱到反倒有些苛求和不妥。

<<Windows取证分析>>

内容概要

本书的写作源于实战的需要，主要关注Windows取证分析这一技术领域，主要讨论了Windows统开机和关机的不同时刻对证据数据收集和分析的技术问题，重点阐述了Windows内存分析、注册表分析、文件分析、可执行文件分析，以及Rootkits等内容。
本书不仅为取证分析人员、调查人员和应急响应人员提供参考，也可为政府和公司的调查人员、司法官员及对Windows取证分析感兴趣的读者提供参考和帮助。

作者简介

Harlan Carvey（CISSP），同时也是《Windows取证和事件恢复》（Windows Forensics and Incident Recovery）一书的作者。
Harlan Carvey是硅谷北部和大都会地区的计算机取证与应急响应顾问，现在他为全美所有地区的客户提供紧急事件响应和计算机取证服务。
Harlan的专业领域

<<Windows取证分析>>

书籍目录

前言第1章 开机取证：数据收集 引言 开机取证（Live Response） 诺卡德交换原理 易变信息的次序 何时进行开机取证 收集什么数据 系统时间 当前登录用户 打开的文件 网络信息（缓存的NetBIOS名字列表） 网络连接 进程信息 进程到端口的映射 进程内存 网络状态 剪贴板内容 服务/驱动信息 命令行历史 映射的驱动器 共享 非易变信息 注册表设置 事件日志 设备和其他信息 有关怎样挑选工具 开机取证方法 本地开机取证方法 远程取证方法 混合方法 小结 参考资料 快速解决方案 常见问题第2章 开机取证：数据分析 引言 数据分析 案例一 案例二 敏捷分析 扩大范围 应对 防范 小结 参考资料 快速解决方案 常见问题第3章 Windows内存分析 引言 内存分析简史 获取物理内存镜像 基于硬件的方案 利用火线接口 崩溃转储 利用虚拟机 休眠文件 DD分析物理内存镜像 进程基础 分析内存镜像 分析进程内存 提取进程可执行文件镜像 内存镜像分析和页交换文件 根据内存镜像判断操作系统类型 分析内存池 获取进程内存 小结 参考资料 快速解决方案 常见问题第4章 注册表分析 引言 注册表内部结构 配置单元文件内的注册表结构 注册表作为日志文件 监视注册表变化 注册表分析 系统信息 自动启动位置 枚举注册表白动启动位置 USB移动存储设备 Mounted Dcvices 查找用户 追踪用户活动 Windows XP系统还原点 小结 光盘内容 参考资料 快速解决方案 常见问题第5章 文件分析 引言 事件日志 理解事件 事件日志文件格式 事件日志头部 事件记录结构 Vista事件日志 IIS 日志 因特网浏览器历史 其他日志文件 回收站 系统还原点 Prefetch文件 快捷方式文件 文件元数据 Word文档 PDF文档 图像文件 义件特征分析 NTFS分支数据流 其他分析方法 小结 参考资料 快速解决方案 常见问题第6章 可执行文件分析 引言 静态分析 记录文件信息 分析可执行文件 动态分析 测试环境 一次性系统 工具 流稗 小结 参考资料 快速解决方案 常见问题第7章 Rootkits及其检测 引言 Rootkits Rootkit检测 开机枨测 GMER Helios MS Strider GhostBuster F-Secure BlackLight Sophos Anti-Rootkit AntiRootkit.com 后期检测 预防 小结 参考资料 快速解决方案 常见问题

章节摘录

第1章　开机取证：数据收集　　引言　　传统调查过程中，传统的方法是现场调查人员直接关闭计算机，然后取得系统硬盘的按位镜像。
这种方法简单实用，但是在当前很多实际的调查过程中却不再适用。
调查人员和应急响应人员发现有些案例中面临的问题，不能通过硬盘镜像找到答案。
例如，在一些通过即时聊天过程诱骗的儿童失踪案中，如何最好地处理证据就是这样一种情形，这种情形在与一些司法官员的交流中也得到了证实。
该问题并不是仅困扰司法人员。
很多案件中，最佳的证据和信息源存在于计算机内存中（网络连接、即时聊天客户端的内容、即时聊天进程的内存数据等），因为一些即时聊天程序客户端并不自动保存聊天记录信息。
另外一些案件中，调查人员需要知道系统中是否有木马或者恶意程序的运行，敏感的数据文件是否从该系统中被复制，在系统运行的时候，到底发生了哪些行为。
技术支持人员通过IDS或者防火墙发现异常／问题流量的时候，经常直接关闭产生这些流量数据的系统，而不管流量数据产生的原因。
类似这些情况，调查人员都需要进行开机取证（live response）——在系统运行的时候收集数据。
开机取证措施也会有一些负面影响，本章将讨论这些问题。

<<Windows取证分析>>

版权说明