第一图书网, tushu007.com

<<计算机取证>>

图书基本信息

书名：<<计算机取证>>

13位ISBN编号：9787111212416

10位ISBN编号：711121241X

出版时间：2007-5

出版时间：机械工业出版社

作者：Dan Farmer何泾沙

页数：186

译者：何泾沙

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

第一图书网, tushu007.com

内容概要

本书以重构过去事件为重点，目的是发现问题、分析问题、解决问题。
本书分三部分，第一部分计算机对所涉及的基本概念进行介绍，包括以后章节中所用到的一些基本技术。
第二部分计算机对文件系统、进程和操作系统的抽象进行了探讨。
第三部分计算机主要对文件、进程和操作系统抽象之外的部分进行探讨。
本书面向那些想深入了解计算机系统的工作原理，以及想学习计算机入侵和系统分析技术的读者，适合计算机系统管理员、安全专家、开发人员等参考。

第一图书网, tushu007.com

作者简介

作者：(美)法默 (美)温玛 译者：何泾沙 等

书籍目录

译者序前言第一部分 基本概念　第1章 计算机取证宗旨　1.1 引言　1.2 突显异常活动　1.3 易失性顺序　1.4 层与假象　1.5 信息的可信度　1.6 被删除信息的固化　1.7 数字考古学与地质学　第2章 时间机器　2.1 引言　2.2 故障的第一个特征　2.3 MAC时间介绍　2.4 MAC时间的局限性　2.5 Argus:情况变得更为复杂　2.6 淘金：在隐蔽的地方寻找时间信息　2.7 DNS和时间　2.8 日志文件系统和MAC时间　2.9 时间的缺陷　2.10 结论第二部分 探讨系统抽象　第3章 文件系统基础　3.1 引言　3.2 文件系统的字母表　3.3 UNIX文件组织结构　3.4 UNIX文件名　3.5 UNIX路径名　3.6 UNIX文件类型　3.7 首次揭密——文件系统内部情况　3.8 UNIX文件系统布局　3.9 揭开秘密——深入探索文件系统　3.10 模糊区——隐藏在文件系统接口之下的威胁　3.11 结论　第4章 文件系统分析　4.1 引言　4.2 初次接触　4.3 准备分析被入侵的文件系统　4.4 捕获被入侵的文件系统信息　4.5 通过网络发送磁盘镜像　4.6 在分析的机器上挂载磁盘镜像　4.7 现存文件的：MAC时间信息　4.8 现存文件的详细分析　4.9 掩盖现存文件分析　4.10 插曲：当一个文件被删除时，将会发生什么？　4.11 被删除文件的MAC时间信息　4.12 被删除文件的详细分析　4.13 利用索引节点号发现异常文件　4.14 追踪一个被删除文件的原始位置　4.15 通过被删除文件的索引节点号来追踪被删除的文件　4.16 回到入侵的另外一个分支　4.17 丧失无辜　4.18 结论　第5章 系统与破坏　5.1 引言　5.2 标准计算机系统结构　5.3 UNIX系统从启动到关闭的生命周期　5.4 案例研究：系统启动的复杂性　5.5 内核配置机制　5.6 使用内核安全等级来保护计算机取证信息　5.7 典型的进程和系统状态工具　5.8 进程和系统状态工具是如何工作的　5.9 进程和系统状态工具的局限性　5.10 用rootkit软件进行破坏　5.11 命令级破坏　5.12 命令级的隐蔽和检测　5.13 库级破坏　5.14 内核级破坏　5.15 内核rootkit的安装　5.16 内核rootkit的操作　5.17 内核rootkit的检测与隐藏　5.18 结论　第6章 恶意攻击软件分析基础　6.1 引言　6.2 动态程序分析的危险　6.3 硬件虚拟机的程序限制　6.4 软件虚拟机的程序限制　6.5 软件虚拟机限制的危险性　6.6 Jails和chroot()的程序限制　6.7 系统调用监控程序的动态分析　6.8 系统调用审查程序的限制　6.9 系统调用哄骗程序的限制　6.10 系统调用限制的危险　6.11 库调用监控的动态分析　6.12 库调用程序的限制　6.13 库调用限制的危险　6.14 机器指令级的动态分析　6.15 静态分析与逆向工程　6.16 小程序存在许多问题　6.17 恶意攻击软件分析对策　6.18 结论第三部分 超越抽象　第7章 被删除文件信息的持久性　7.1 引言　7.2 被删除信息持久性举例　7.3 测量被删除文件内容的持久性　7.4 测量被删除文件MAC时间的持久性　7.5 被删除文件MAC时间的强力持久性　7.6 被删除文件MAC时间信息的长期持久性　7.7 用户活动对被删除文件的：MAC时间信息的影响　7.8 被删除文件信息的可信度　7.9 为什么被删除文件信息能够保持不变　7.10 结论　第8章 超越进程　8.1 引言　8.2 虚拟内存的基础知识　8.3 内存页的基础知识　8.4 文件和内存页　8.5 匿名内存页　8.6 捕获内存　8.7 savecore命令　8.8 静态分析：从文件中识别内存　8.9 在无密钥的情况下恢复加密文件的内容　8.10 文件系统块VS.内存分页技术　8.11 识别内存中的文件　8.12 动态分析：内存数据的持久性　8.13 内存中文件的持久性　8.14 非文件或匿名数据的持久性　8.15 交换分区的持久性　8.16 引导进程内存的持久性　8.17 内存数据的可信度和坚韧性　8.18 结论附录A Coroner's工具包及其相关软件附录B 数据收集和易失性顺序参考文献

编辑推荐

Dan Farmer，撰写过许多计算机安全方面的程序和论文。
他目前在Elemental Security公司任首席技术执行官，该公司是一家计算机安全软件公司。
Wietse Venema曾经编写了一些得到广泛应用的软件，包括TCP包装软件以及Postfix邮件系统。
他目前在IBM研究部门任研究员。
两位作者还合作编写了很多国际领先的信息安全和取证方面的软件程序包，包括SATAN网络安全扫描程序以及Coroners工具包。

第一图书网, tushu007.com

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