"已出版的最全面的应急响应指南"

——Marc J. Zwillinger 前美国司法部计算机犯罪和知识产权科法律代理人

应急响应

计算机犯罪调查

[美] Kevin Mandia
Chris Prosise 著

常晓波 译

Mc Graw Hill

清华大学出版社

应急响应

计算机犯罪调查

[美] Kevin Mandia
Chris Prosise 著
常晓波 译

清华大学出版社

(京)新登字 158 号

应急响应:计算机犯罪调查

Kevin Mandia Chris Prosise : Incident Response: Investigating Computer Crime

EISBN: 0-07-213182-9

图书在版编目(CIP)数据

应急响应:计算机犯罪调查/(美)曼迪亚,(美)普罗西思著;常晓波译. —北京:清华大学出版社,2002

书名原文:INCIDENT RESPONSE: INVESTIGATING COMPUTER CRIME

ISBN 7-302-05730-3

Ⅰ. 应… Ⅱ. ①曼…②普…③常… Ⅲ. 电子计算机—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2002)第 059148 号

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)

http://www.tup.tsinghua.edu.cn

责任编辑:付宇光

封面设计:郑 晶

版式设计:肖 米

印 刷 者:清华大学印刷厂

发 行 者:新华书店总店北京发行所

开 本:787×960 1/16 **印张**:31.75 **字数**:591 千字

版 次:2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷

书 号:ISBN 7-302-05730-3/TP·3382

印 数:0001~4000

定 价:63.00 元

译者序

随着计算机技术与网络技术的逐渐成熟和推广，可以说计算机犯罪到了日益猖獗的地步。在发生了突发事件之后，经常需要及时恢复受危及的系统、寻找攻击者的蛛丝马迹、获取黑客的犯罪证据、为诉诸法律做好一切准备。所有这些工作，都是本书研究和介绍的内容。本书不仅仅提供了对付突发事件的应急响应所需的技术细节，还为读者提供了解决突发事件所需要考虑的重要事项。

本书总共分为5个部分：第1部分讲述了应急响应的基础；第2部分研究了应急响应的技术细节，包括关于如何制定策略的指导、司法鉴定过程，以及在应急响应过程中涉及的各种网络技术综述；第3部分讨论了针对Windows NT、Windows 2000、UNIX（Linux、Solaris及其他系统）等操作系统的突发事件和初始响应以及调查过程；第4部分讨论了对最流行的Web服务器攻击、路由器攻击和应用程序服务器攻击的响应。最后的附录部分提供了更多的背景资料和相关信息，包括一些应急响应组织和法律条文。本书对于计算机网络安全工作者和有志于从事网络安全工作的人来说是一本价值极高的必备参考书。

参加本书翻译的人员有常晓波、朱剑平、栗庆丰、刘颖等。常晓波对全书进行了初步的校对工作，马睿倩做了初步的排版工作。在此，谨向为本书出版付出辛勤劳动的所有人致

以诚挚的感谢！

在与清华大学出版社计算机引进版图书编辑室合作的过程中，出版社的朋友们一丝不苟的工作态度使我们受益颇多。在此，致以诚挚的谢意！

由于我们水平有限，书中难免会出现一些错误，真诚欢迎各界朋友批评指正。

译　者

2001 年 9 月于北京

本书献给那些没有经过培训的、没有时间的、必须使用落后的设备仔细检查大量数据的执法人员。

——作者

献给我的妈妈 Diane Heckathorne，有一天在我没有教会她如何使用电子邮件时，她很平静地提醒我说："不要忘了是我教你说话的"。我马上就恢复了耐心。

——Kevin Mandia

献给我的妻子 Emily，感谢她对我的耐心和鼓励。另外还要献给我的爸爸，感谢他对我的关心和支持。最后还要献给 Butterwood。

——Chris Prosise

关于作者

◇ Kevin Mandia

Kevin 是一家名为 Foundstone 的互联网安全公司的计算机司法鉴定主管，并且是一位著名的司法鉴定和应急响应专家。作为一名特殊的代理人、顾问和讲师，Kevin 积累了丰富的经验和专业技术。

Kevin 讲授应急响应方面的问题已经有很长的历史，曾经专门为 FBI 编写过为期两周的计算机入侵响应课程和为期一周的高级网络调查课程。Kevin 曾经在 Quantico 市（隶属于美国弗吉尼亚州）讲授过一年多的课程，有将近 340 名 FBI 人员专门参加了他的有关计算机入侵的课程。课程的内容是为满足执法人员、情报人员和那些必须理解计算机网络操作方式和黑客滥用网络资源的方法的个别人的特殊需要而量身定制的。

Kevin 还曾经为来自美国国务院、美国中央情报局（CIA）、美国国家宇航局（NASA）、Prudential、SIAC 和美国空军的成员进行过关于计算机入侵方面的培训。Kevin 曾经为 FBI 的美国国家基础设施保护中心（National Infrastructure Protection Center）、美国空军特殊事件调查科（Air Force Office of Special Investigations）、某些公司实体和州立执法机关提供调查支持。他还编写过司法程序、宣誓书，并开发过专门用于电子跟踪和捕获计算机黑客的特殊软件。

Kevin 是一名活跃的演讲者，每年都会在许多会议和活动中进行演说。他获得了 Lafayette College 的计算机科学学士学位和 George Washington University 司法鉴定科学的硕士学位，并且是美国空军特殊事件调查科（Air Force Office of Special Investigations）的预备军官。

◇ Chris Prosise

Chris Prosise 是 Foundstone 公司专业服务部的副总裁，该部门提供计算机安全咨询和培训服务。Chris 在攻击和渗入测试以及应急响应方面具有丰富经验。他领导的政府和商务安全任务团队，在世界范围内开展从拥有最高机密性的政府网络的敏感性应急响应任务，到某

些世界级大公司的全面安全评估的工作。

作为 Foundstone 公司的创始人之一，Chris 为政府和商业公司开发并讲授过关于应急响应、黑客入侵和网络安全的课程。Chris 具有重要的工具开发经验，曾经为美国空军开发过自动扫描工具和实时入侵侦测与防范软件，他是从美国国家信息战中心空军办公室（Air Force Information Warfare Center）作为现役官员开始了自己的信息安全职业生涯。

Chris 在诸如 Networld Interop、SC Magazine 的 Securing the E-Business 和 Forum of Incident Response and Security Teams（FIRST）等会议上是个十分活跃的演说家。他还经常为杂志撰写文章，而且是 CNET 上定期安全专栏“Security Issues”（http://builder.cnet.com）的固定撰稿人。

Chris 获得了 Duke University 的电子工程学士学位，和 Certified Information Systems Security Professional（CISSP）认证。

关于撰稿作者

◇ Matt Pepe

Matt Pepe 是美国最有经验的应急响应专家之一，曾经为美国空军特殊事件调查科、FBI 和其他政府机构的 100 多次联合调查执行过司法鉴定分析。他还是一位很成功的信息安全顾问，经常领导网络评估，并且从事攻击和渗入交战的工作。Matt Pepe 的联系方式为：matt@incidentresponsebook.com。

关于技术编辑

◇ Clinton Mugge

Clinton Mugge 在过去的 7 年间在 IT 安全领域从事入侵和渗入测试的工作。他服务于一家反智能犯罪机构，负责执行涉及机密和非机密的政府网络的应急响应和计算机调查。在全世界，Mugge 先生曾

经成功地对包括全球财富500强在内的公司的突发事件做出了正确的应急响应，并开发了全面的应急响应程序。Mugge先生常常在很多会议上发表演说，并为司法鉴定和应急响应队伍服务。

◇ Mike Shema

Mike Shema是Foundstone公司的首席顾问，在该公司中，还与他人合作开发并讲授应急响应和安全课程。曾经为金融、IT和政府客户执行过许多次安全渗入和应急响应交战。Mike Shema是一位资深的程序员，曾发现了0天滥用现象(zero-day exploits)并倡导了Web应用程序测试方法论。Shema先生获得了Penn State的电子工程专业的学士学位。

致 谢

在此要感谢一些朋友，如果没有他们的帮助和影响，本书不可能完成。感谢 Doris 和 Gary Gardner，是他们展开了这个极大的工程并把我们组织在一起；感谢 Curtis Rose，他是我们见过的最有条理最谨慎的调查员；感谢 Scott Larson、Scott Crabtree 和 Chris Wrobleski，他们提供了自己的案例并付出了大量的劳动；Ed Stroz 指导我们相互信任、团结一致；Keith Jones、William Chan、Clinton Mugge、Mike Shema 和其他工作人员在我们出差和写作时做了大量具体的工作，感谢你们；Lt. Col. Anne Burtt（已退休）给我们作出了榜样，教会我们如何用最少的力气做更多的事，感谢您；Matt Pepe 是一个耐心而且严厉的人；Joel Garmon 和 Ron Nguyen 来自空军信息战中心（AFIWC），给予我们很多耐心的指导，感谢你们；感谢 1988 Lafayette 橄榄球队的教练组；感谢 Michele Dempsey 的等待；感谢 James Buffet 的观点；感谢 Daves Poplar 和 Lafalce，虽然他们没有为本书做任何工作。

我们还要感谢新奥尔良的 C. J. Moses、Brian Hutchison、Jack Wiles、John Patzakis、Shawn McCreight、Joe Zagorski（主力成员）、Marc Zwillinger、Big Sid 和 Will，联邦调查局（FBI）、空军特别调查局（AFOSI）及空军计算机应急响应队伍（AFCERT）的 Trent Teyema、

Dave Vanzant 和所有其他为我们提供指导的人们。我们希望有一天能够回报你们的帮助。

最后还要感谢为本书的完成付出了巨大努力的 Osborne 全体工作人员。我们由衷地感谢 Jane Brownlow、Emma Acker、Carolyn Welch、Ross Doll、Marilyn Smith、Lisa Theobald 以及其他有关人员。

前　言

任何阅读过2001年美国联邦调查局(FBI)和计算机安全协会年度调查的人都会得出一个无法避免的结论:计算机犯罪的确存在。无论是政府机构,还是大中型或小型公司,甚至是使用家庭Internet宽带网络在家中工作的人,都可能成为攻击的目标。在最近对超过500人的不同群体所作的关于计算机犯罪的研究表明,85%的答复者承认曾经由于计算机安全漏洞而遭受损失。调查答复者在5年中可估算的损失超过10亿美元的情况还是第一次出现。

今后,所有拥有Internet站点的组织都有可能成为某种计算机突发事件的受害者,因此学习如何应付这种突发事件是很关键的,对网络攻击做出适当的响应是一件很难的任务。虽然受到攻击的可能只是计算机系统,但因为计算机应急响应所涉及的不仅仅是技术问题,所以有效的响应必定要涉及多个学科。正确的计算机应急响应必然要涉及法律方面的分析,并有可能引起一些间接性问题,这些问题需要借助传媒和股东关系、保险专家的帮助得以处理,最终还需要公司高层人士进行裁决。

对于任何类型的恶意突发事件,必须要在攻击发动前抵制攻击并确定罪犯。在这一点上,正确的规划是十分关键的。一旦发生了恶意的突发事件,就要做出迅速和深思熟虑的响应以防止更大的损失,并要找出足够的证据以追踪和确定罪犯。虽然任何接受过司法鉴定培训的调查员都可以找出罪犯存储在PC上的证据,但更为需要的是对网络攻击做出迅速、深思熟虑的响应所需的经验。能够以一种可保留所有

用于司法鉴定的相关证据的方式执行响应，同时又能够高效评估攻击的性质、攻击者的技能以及所带来的损害的人真是少之又少。本书的作者正好是这方面的专家，曾经为政府部门和私营公司的网络处理过大范围的计算机应急响应。将这些综合起来，本书就成为已出版的应急响应领域的最精确最全面的指导手册。

本书的与众不同之处还在于作者不仅提供了技术细节，还提供了相关的法律环境用于理解如何通过一种很实际的方法高效地解决突发事件。因此，无论读者的技术经验如何，本书都是很有价值的。除了对一次全面攻击进行应急响应的详细操作步骤指导之外，本书还提供了突发事件的实际例子，这些实例是以前政府部门和私营公司调查过的案件，包括对这些案件中所使用的应急响应技术是否有成效的分析。

虽然实际经验无可替代，但本书对于那些对付计算机攻击的人员而言仍然是一本必备的参考价值极高的书。应该在恶意突发事件实际发生之前仔细阅读本书，并在受到不可避免的攻击时将本书作为参考。

Marc J. Zwillinger

Marc J. Zwillinger 是位于美国华盛顿特区的 Kirkland & Ellis 公司的股东，并且是公司的计算机法律与信息安全部(Cyberlaw and Information Security Practice)的负责人。在加入 Kirkland & Ellis 之前，他是美国司法部计算机犯罪与知识产权科(United States Department of Justice Computer Crime & Intellectual Property Section，CCIPS)的实习律师。在 CCIPS 任职期间，Zwillinger 先生率领 DOJ 律师小组负责调查计算机入侵案件，包括 2000 年 2 月电子商务网站爆发的拒绝服务攻击。现在，Zwillinger 先生通过制定预防策略并对电子攻击和专有信息的盗取进行内部调查，通过自己的经验帮助公司防止、最小化和补偿计算机突发事件所造成的损失。他在天主教大学(Catholic University)的哥伦布法学院(Columbus School of Law)担任计算机法律的副教授。同时还是 Foundstone 公司(www. foundstone. com)的法律讲师，讲授题目为《Understanding Cyber Attacks: Hands-on》的培训课程。

简 介

您一定对应急响应感兴趣！当您希望了解应急响应的时候，首先需要一本类似于本书的拥有大量技术细节的书籍。应急响应是计算机安全的一个新兴知识领域，其内容是非常吸引人的。在该领域中，非法律界人士要履行许多传统司法部门的职责。公司雇员和大学生们不会去处理凶杀案件的证据，这也不是他们的责任。但是必须允许计算机犯罪的受害者恢复受危及系统、设置安全防护措施并处理犯罪的电子证据。系统管理员要查阅雇员的电子邮件、监视网络流量、检查入侵探测系统、监视基于主机的日志记录，并确保雇员没有用公司的网络制造计算机恶作剧。因此，系统管理员现在已经成了“网络警察”，并在计算机犯罪发生时展开初步调查。这可不是一项简单的工作，数字证据比其他任何类型的证据更容易被篡改、破坏或藏匿。本书旨在培训系统管理员对计算机犯罪作好准备，并综合了应急响应所需的调查、司法鉴定和相关技术知识。

我们为什么要编写这本书

本书介绍了调查计算机安全突发事件的专业方法。在调查计算机安全突发事件期间，未经训练的系统管理员、司法部门官员或计算机安全专家可能会在无意中破坏有价值的证据，或者发现不了非法或者未授权活动的重要线索。缺乏培训会大大地削弱缉拿来自外部和内部的攻击者的能力。我们亲眼目睹了许多计算机司法鉴定，从深奥的技能到专利的机密技术，几乎每家从事司法鉴定分析的公司都开发了许多

自己的工具，但并不将它们共享使用。同样，大量的司法鉴定培训是针对司法部门的人员的，尽管对安全突发事件的大部分初步响应都是由系统管理员完成的。他们非常普通而且经常过度操劳，却得不到有效的培训。因此，本书提供了详尽的技术案例，示范如何进行计算机司法鉴定和分析。网上有许多在线刊物和书籍提供了一些关于应急响应的培训和指导，但它们通常是分散的、过期的，根本无法应付当前计算机犯罪的挑战。

作者的注释

在本书中，我们特地使用安全性突发事件（security incident）这个术语来指在计算机介质（或在内存）中留下证据的劣行，而没有采用计算机犯罪（computer crime）这个词。其原因有两方面：并不是每个事件都会构成计算机犯罪，而计算机犯罪这个术语意味着司法部门的介入。然而对于许多突发事件，公司会采取有效的方式悄悄地进行内部处理。

哪些人应该阅读本书

如果您在凌晨两点被电话叫醒，因为有人“黑”了您的 Web 页面，那么本书就很适合您。如果主管要求调查是否有雇员将公司的机密发送给公司的竞争对手，则本书也适用您。如果有用户惊慌失措地告诉您，他的计算机崩溃了，那么本书可能对您也有所帮助。如果需要处理以下事情，本书也将提供详尽、法律上适当的技术支持。

- ▼ 调查偷窃源代码或机密信息的行为
- ■ 调查偷窃密码文件或信用卡信息的行为
- ■ 调查垃圾邮件或电子邮件的骚扰和恐吓
- ■ 调查计算机系统的越权或非法入侵
- ■ 调查拒绝服务攻击
- ■ 为犯罪、诈骗、谍报和安全性的调查提供司法鉴定
- ■ 作为公司计算机突发事件和计算机司法鉴定事务的关键人物
- ▲ 为计算机搜查和捉捕提供在线援助

使用便于阅读的独特图形元素

图标

下列图标代表您将在本书中看到的标题：

可能发生的事情

我们简要地描述了可能发生的突发事件。在每个突发事件之后，我们会向您说明如何作出响应或到何处去寻找证据，后者有其专用图标：

到何处去寻找证据

直接去找所需的证据！

司法部门提示

该图标代表司法部门人员所提供的内部提示，这些提示对美国公司大有裨益。

我们还大量使用了增强视觉效果的图标，以突出那些需要注意的细节：

注意

警示

本书对应的 Web 站点亦是本书的一个重要组成部分，我们在每个涉及 www.incidentresponsebook.com 的地方创建了一个图标。

方框元素

除了上述图标，我们在书中还大量使用了方框元素和线条元素。

目击者报告

我们描述了在现实生活中曾经亲自调查的突发事件，并给您提供解决方案的内部信息。

犯罪行为　请勿效仿　　犯罪行为　请勿效仿　　犯罪行为　请勿效仿

我们通过描述细节情景建立起犯罪场景，就好像它们真实地发生在您周围。这与前面提到的“可能发生的事情”有所区别，因为它提供了更为详细的场景。

从 Web 上获取有关资料

这代表正文中的一组 Web 地址引用。

最后，在每章结尾有一个“结束语”部分。这是将本章节全部内容贯穿在一起的总结，并说明了所讨论内容的重要性。

本书的组织结构

本书介绍了解决突发事件的一整套连贯方法，从对付突发事件的准备到详细的技术响应面面俱到。这套方法阐明了围绕突发事件解决方案的法律问题和制定决策的过程。此外，在本书开始，我们提供了调查当今应用最普遍的操作系统和应用程序所必需的具体技术步骤。在整本书中我们还使用了现实生活中自己亲身经历的案例，力争构成一个鼓励创造性地解决司法鉴定问题的环境。

- **第 1 部分** ***初步了解：应急响应的基础***

“初步了解”通过案例和方法论建立起应急响应的基础。这部分将现实生活中的经历和结构化的方法论相结合，以便读者对计算机安全性突发事件的彻底理解。在这部分中还讨论了一个公司如何提高应急响应能力，以此成功地保护其资产。我们讨论了会见过程，应该通知哪些人，以及如何快速地确定调查的范围。

- **第 2 部分** ***全力出击：学习技术细节***

这部分介绍了计算机司法鉴定的全部过程。我们为司法鉴定分析提供了详细的技术，并回答了许多问题，例如是要以逐字节的物理方式复制系统，还是要从逻辑上复制文件。我们讨论了证据标准的重要性和证据的存储及处理，然后详细地介绍了硬盘驱动器的司法鉴定复制技术，以及在司法鉴定分析过程中所使用的工具。我们逐步介绍了安置网络窃听器的技术细节。

- **第 3 部分和第 4 部分** ***调查系统和非特定平台的技术***

当我们作为面红耳赤的官员开始调查计算机犯罪时，面对受危及系统会不知所措，因为我们不能确定采取什么措施最合适。本书的第 3 部分和第 4 部分提供了确认和调查突发事件所必需的技术细节，即一本几年前就需要的手册。我们提供了大量“可能发生的事情”的情景，描述了许多现实生活中的攻击方法。然后阐述了“到何处去寻找证