科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

虚拟安全

沙盒、灾备、高可用性、取证分析和蜜罐

John Hoopes, Aaron Bawcom, Fred Shore, Paul Kenealy, Andreas Turriff
Wes Noonan, Carsten Willems, Craig Schiller, David Williams 著
杨谦 谢志强 译

Virtualization for Security
Including Sandboxing, Disaster Recovery, High Availability,
Forensic Analysis and Honeypotting

科学出版社

Virtualization for Security

Including Sandboxing, Disater Recovery, High Availability, Forensic Analysis and Honeypotting

虚拟安全

沙盒、灾备、高可用性、取证分析和蜜罐

John Hoopes
Aaron Bawcom
Paul Kenealy
Wes Noonan
Craig Schiller
Fred Shore
Andreas Turriff
Carsten Willems
David Williams
著

杨 谦 谢志强 译

科学出版社

北 京

图字：01-2010-2757 号

Virtualization for Security：Including Sandboxing, Disater Recovery, High Availability, Forensic Analysis and Honeypotting
John Hoopes, et al.
ISBN-13: 9781597493055

Authorized Simplified Chinese translation edition published by the Proprietor.
ISBN:9789812727046

图书在版编目（CIP）数据

虚拟安全：沙盒、灾备、高可用性、取证分析和蜜罐/(美)胡普斯(Hoopes,J.)等著；杨谦，谢志强译. —北京：科学出版社，2010

ISBN 978-7-03-028453-2

Ⅰ. ①虚… Ⅱ.①胡…②杨… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 147031 号

责任编辑：田慎鹏 霍志国 杨 然／责任校对：张怡君
责任印制：钱玉芬／封面设计：耕者设计工作室／封面图片：徐湛

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销
*
2010 年 8 月第 一 版 开本：787×1092 1/16
2010 年 8 月第一次印刷 印张：16
印数：1—4 000 字数：376 000

定价：46.00 元

（如有印装质量问题，我社负责调换）

译 者 序

新形势下如何高效地解决网络安全问题，成为摆在众多实验室和公司面前的一道难题。虚拟化技术不仅可以应用在数据中心提高资源的利用率、系统的可用性，也可以用在网络安全研究和实施中。本书就是这样一本关于虚拟化在信息安全中使用的指南。

本书特色鲜明，不仅是工程技术人员的工具书籍，也是公司信息化管理者的参考书籍。本书全面细致、重点突出地介绍了虚拟化技术的起源和现有主要类型，并对各主要类型进行比较，可作为数据中心选型的重要参考，也使得工程技术人员进一步看清虚拟化技术的发展方向。本书也是网络安全研究人员的知音，因为它介绍了最新的虚拟化在安全研究中如何使用并给出很多实例，这不仅可以使很多研究人员告别以前陈旧的实验方法提高研究速度与效果，也推广了许多新的安全研究方法，例如沙盒、恶意软件分析等。本书也可作为新时期法官和律师的参考书，因为随着网络的广泛应用，许多案件证据涉及计算机取证，如何把握计算机取证，是法官和律师需要面对的问题，本书深入浅出地介绍了计算机取证的知识。

翻译国外作品，一边是感到万分荣幸，一边也是兢兢小心。对于本书这样的最佳安全研究与实践之作，即便是需要兢兢业业，也是值得翻译的。一直到现在，依然有很多资深的开发人员对虚拟化认识有所局限。包括译者在内，虽然每日都在使用虚拟机，但是对虚拟化的作用还是认识不足。但即便如此，业内人士也不得不承认，虚拟化正日益成为数据中心和开发测试研究以及其他应用的发展趋势。

本书承载的内容丰富而深入。翻译的过程中译者也常感汗颜，原来自诩对计算机安全颇为了解的我深刻感受到自己知识面的浅薄和不完整，于是翻译的过程也成为了自己检讨和学习的过程，收获颇丰。本书的作者都是计算机安全方面的知名研究者，有些是业内开源项目的领导者或者资深工程师，书中的很多内容都是他们长年实践的经验心得。希望大家反复阅读，必定受益无穷。由于本书作者的知识广博，经验丰富，而译者本人知识有限时间仓促，难免对作者的个别匠心无法原汁原味地呈现，在此敬请各位读者多多包含，不辞吝教，指出纰漏。我也希望能就本书的内容与读者有更多的交流，我的邮箱是 yqbjtu@live.com。

最后，我要感谢科学出版社的霍志国编辑在译书的过程中给我们的莫大帮助，还要感谢我的朋友华北计算技术研究所的雷昕、李晓亮、杨艳、刘争涛、吴林、杨建轩、尹相乐、武严严和东莞经济贸易学校的谢志强老师。当然，还有一位是一定要特别感谢的，正是边的不断督促，才使我按时保质完成翻译。

杨 谦

2010 年 7 月于北京志新村

技术编辑

John Hoopes 是 VeriSign 公司的高级咨询师。他的专业背景包括 IBM AS/400、IBM 巨型机(OS/390 和 Z 系列)、AIX、Solaris、Windows 和 Linux 许多不同平台的操作/支持工作。John 的安全专业主要集中在应用软件测试，重点是逆向工程和协议分析。在做咨询师之前，John 是一名 IBM 的应用系统安全测试组组长，负责安全服务部署、外部服务交付以及工具开发。John 同时也负责组员在网络渗透和脆弱性分析方面的培训和指导工作。作为咨询师，John 为零售业、交通运输业、电信业和银行业的客户做一些安全合同方面的工作。John 毕业于犹他州立大学。

John 对第 4 章有所贡献，撰写了第 6～8，12 和 14 章。John 也对第 3，10 和 11 章进行了技术编辑。

贡 献 者

Aaron Bawcom 是 Reflex 安全公司的工程部副总裁。Reflex 安全公司的主要业务是帮助一些公司加速采用下一代虚拟数据中心。在 Reflex 公司，Aaron 推动领导虚拟化市场的技术创新。他也对下一代管理、虚拟化、云计算以及应用感知网络技术进行架构设计工作。在职业生涯中，他设计过防火墙、入侵检测/防御系统、防病毒软件、防间谍软件、用户识别卡、拒绝服务攻击、邮件加密和数据泄漏防御系统。

Aaron 是 Intrusion.com 的 CTO，也是 Network Associates 公司的网络安全部门的首席架构师。他拥有得州农工大学的计算机科学学士学位，当前生活在佐治亚州的亚特兰大。

Aaron 撰写了本书的第 2 章。

Pual Kenealy（俄罗斯与苏维埃研究学学士，红帽认证工程师-RHCE） 他刚完成在皇家霍洛威学院的信息安全硕士学业，现在是位于伦敦金丝雀码头的巴克莱银行的信息安全事件反应处理员。他的专业特长包括有关 Linux 网络服务器、入侵检测和网络架构设计安全。Paul 是 Logica 公司的一名程序员，设计和实现了很多 VMware infrastructure 系统的安全监控和事件分析项目。

Paul 撰写了本书的第 5 章。

Wesley J.Noonan（VMWare 认证专家-VCP，国际注册信息系统审计师-CISA） 是 NetIQ 的一名虚拟化、网络和信息安全领域的专家。在 NetIQ，他直接与客户打交道，理解和满足客户的需求，将自己的经验和 NetIQ 的发展统一起来。Wesley 从事 IT 工作超过 14 年，专长在基于 Windows 的网络和网络基础设施安全设计及实施方面。

Wesley 是持续的业界贡献者，出版了 *Hardening Network Infrastructure*，与人合著了 *Hardening Network Security*，*CISSP Training Guide* 和 *Firewall Fundamentals*，同时是思科网络的 *Hacking Exposed* 的技术编辑。此前，Wesley 出席过 WMworld 2008、TechMentor 和 Syracuse VMUG 大会；在微软认证培训中心授课；开发和交付自己的思科培训课程。他对顶级的业界出版物也有所贡献，如《金融时报》（*Financial Times*），*Redmond Magazine*，*eWeek*，*Network World* 和 TechTarget 的分支机构。

Wesley 与家人目前生活在得克萨斯州的休斯顿。

Wesley 撰写了本书第 10 和 11 章，对第 5 章内容有所贡献，对第 2，4～9，12，13 和 14 章进行了技术编辑。

Craig A.Schiller（CISSP-ISSMP 信息系统安全管理专家,ISSAP 信息系统安全架构

专家） 是波特兰州立大学的首席信息安全官、波特兰社区大学的数字取证分析学兼职讲师、衣阿华安全培训有限公司的总裁。他是 *Botnets: The Killer Web App*（Syngress, ISBN: 1597491357）的第一作者，第一位 GSSP（generally accepted system security principles）。他是多版 *Handbook of Information Security Management* 和 *Data Security Management* 的贡献者。Craig 也是 *Infosecurity 2008 Threat Analysis*（Syngress, ISBN: 9781597492249），*Combating Spyware In The Enterprise*（Syngress, ISBN: 1597490644），*Winternals Defragmentation, Recovery, and Administration Field Guide*（Syngress, ISBN: 1597490792）的贡献者。

Craig 是一名高级安全工程师，参与美国国家宇航局 AIS 安全工程的架构设计。与人合作创建了两个美国信息系统安全协会的地方分会：中央平原分会和得克萨斯州墨西哥湾海岸分会。 目前他是信息安全协会-波特兰的教育主任，也是俄勒冈州希尔斯伯勒警察局特约专家。

Craig 是路易斯安那州拉斐特（Lafayette）人。目前与妻子 Janice 和家人（Jesse，Sasha 和 Rachael）居住在俄勒冈州比弗顿。Janice 和 Craig 与圣塞西莉亚大教堂的“棒极了”唱诗班一起唱歌。

Craig 对第 3 章内容有所贡献，撰写了第 9 章。

Fred Shore（Healthcare Partners Medical Group） 是 Healthcare Partners 医疗集团的客户支持分析师。他提供基于 Windows 操作系统的专业支持。他的 Windows 系统专长来源于 17 年多的技术支持经验。他的背景包括广泛的发现问题并解决问题的能力，也包括在北美信息技术和维旺迪游戏公司（Vivendi Games）以及波特兰州立大学办公室的期间练就的节省开支能力。

Fred 拥有商业管理学士学位：波特兰州立大学信息系统。他目前与他的狗 Chance 生活在南加利福尼亚。

Fred 对本书第 3 章内容有所贡献。

Andreas Turriff（MSCE，MCSA，CNE-5，CNE-6，MCNE） 是波特兰州立大学 IT 安全组的成员，为首席信息安全官工作。Craig Schiller，Andreas 为计算机取证分析整合了一些工具，将其放在可启动的媒体上以供内部使用；他当前的主要工程是开发一个启用了二进制和内核级别加固的 Linux Live-DVD，以确保取证分析工具在恶意软件分析时的真实性。Andreas 目前是波特兰州立大学大四学生，他正在攻读计算机科学学士学位。此前，他曾做过很多公司的网络管理员。

Andreas 对本书第 3 章内容有所贡献。

Mario Vuksan 是 Bit9 的研究主任。在 Bit9，他帮助创建世界上最大的关于软件的行动情报集合，Bit9 全球软件注册处。他在业界大会上代表 Bit9，当前工作是开发公司的下一代产品和技术。在加入 Bit9 之前，Vuksan 是 Groove Networks 公司（已被微软收购）的项目经理和咨询工程师，Groove Networks 公司的主要业务是基于 Web 的解决方案、P2P 管理和综合服务器。在加入 Groove Networks 前，

Vuksan 在 1414c 开发了第一批 Web 2.0 应用系统，来源于 PictureTel 的 spinoff 原型系统。他拥有斯沃斯莫尔学院的学士学位和波士顿大学的硕士学位。2007 年，他在 CEIC、黑帽大会（Black Hat）、Defcon 黑客大会（Defcon）、防病毒研讨会（AV Testing Workshop）、病毒公报（Virus Bulletin）和亚洲反病毒大会（AVAR）大会上做过发言。

Mario 撰写了本书第 13 章。

Carsten Willems 是一名有 10 年经验的独立软件开发者。他的兴趣在于开发一些与恶意软件研究相关的安全工具。他是自动化恶意软件分析工具 CWSandbox 的创建者。这个工具是他在德国亚琛理工大学攻读计算机安全专业的硕士论文的一部分，这一工具由位于佛罗里达州克利尔沃特的 Sunbelt 软件发布。他目前正在曼海姆大学撰写博士论文《*Automatic Malware Classification*》。2006 年 11 月，他因论文《*Automatic Behavior Analysis of Malware*》获得国际应用安全技术论坛第三名（Competence Center for Applied Security Technology，CAST）。此外，Carsten 也创建了几个办公和电子商务产品。最近，他开发了 SAGE GS-SHOP，一个服务器/客户端在线购物系统，这个系统已经被安装了 1 万多次。

Carsten 对本书第 3 章内容有所贡献。

David Williams 是位于佐治亚州亚特兰大的专业高效企业基础设施解决方案的咨询公司 Williams&Garcia 有限公司的负责人。他的特长在于为 X86 和 X64 环境交付高级解决方案。因为 David 关注成本控制和复杂性化约，所以虚拟化技术在他推荐的解决方案和基础设施设计中扮演着重要角色。David 帮助多个公司的 IT 管理层人员，他的职责包括为 Windows、开放系统、巨型机、存储、数据库和数据中心提供技术以及服务的操作和策略。他同时也以高级架构师和咨询工程师的身份服务于财富 100 强公司，为一些新的企业级工程提供关于技术基础设施的战略方向咨询。

David 曾在迈阿密大学学习音乐工程技术，他拥有 MCSE+I，MCDBA，VCP 和 CCNA 认证。闲暇时，他与妻子和三个孩子一起度过时光。

David 撰写了本书第 1 章。

目　录

Chapter 1

第1章
虚拟化介绍

本章主要内容：

- 什么是虚拟化？
- 为什么要虚拟化？
- 虚拟化是如何工作的？
- 虚拟化类型
- 虚拟化常见用例

☑ 总结
☑ 内容快速回顾
☑ 常见问题