

<<网络安全事件响应>>

图书基本信息

书名：<<网络安全事件响应>>

13位ISBN编号：9787115102041

10位ISBN编号：711510204X

出版时间：2002-5

出版时间：人民邮电出版社

作者：(美)e. eugene schultz russell shumway

页数：247

字数：395000

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>

<<网络安全事件响应>>

内容概要

本书是指导网络与系统安全事件响应工作的一本宝贵的战略指南。

全书首先介绍了事件响应、风险分析等概念及其相关概念之间的关系，然后对事件响应组的组建和管理、时间响应的组织提出了许多建设性的建议，提出了事件处理经典的六阶段方法。

从技术方面描述了入侵跟踪技术、陷阱与诱骗技术、内部攻击的响应问题，并用三章的篇幅介绍了法律问题和取证问题，讨论了事件响应中的人性因素，最后讨论了事件响应的发展方向。

本书适合计算机系统、网络与信息安全的管理人员、技术人员，大专院校从事网络安全技术的研究生、教师等研究人员。

特别是对于计算机安全事件响应组(CSIRT)、安全服务企业以及政府相关的管理部门，本书是市面上难得的一本战略指南。

<<网络安全事件响应>>

作者简介

E.Eugene Schultz博士，美国能源部门的计算机事件咨询能力（CIAC）组的创始人和前任负责人，目前受聘于加州大学的Lawrence Berkeley国家实验室，并在加州大学任都教。

Russell Shumway曾担任Global Integrity公司REACT计划的技术负责人，负责向美国和欧洲的大型商业客户提供事件响应服务，他为Global Integrity公司金融服务事件共享和咨询中心（FS/ISAC）的设计和开发提供了帮助。

<<网络安全事件响应>>

书籍目录

第1章 事件响应简介 1.1 什么是事件响应 1.2 事件响应的基本原理 1.3 事件响应概述 1.4 小结第2章 风险分析 2.1 关于风险分析 2.2 与安全相关的风险类型 2.3 安全事件的数据获取 2.4 紧急响应中风险分析的重要性 2.5 小结第3章 事件响应方法学 3.1 使用事件响应方法学的原理 3.2 事件响应的6阶段方法学 3.3 建议 3.4 小结第4章 事件响应组的组建和管理 4.1 什么是事件响应组 4.2 为什么要组建事件响应组 4.3 组建响应组的问题 4.4 关于事件响应工作的管理 4.5 小结第5章 事件响应的组织 5.1 有效的团队——确保可用性 5.2 训练团队 5.3 测试团队 5.4 成功的障碍 5.5 外部协作 5.6 管理安全事件 5.7 小结第6章 网络攻击的追踪 6.1 什么是追踪网络攻击 6.2 不同环境下的攻击追踪 6.3 追踪方法 6.4 下一步 6.5 构建“攻击路径” 6.6 最后的忠告 6.7 小结第7章 法律问题 7.1 美国有关计算机犯罪的法律 7.2 国际立法 7.3 搜查、没收和监控 7.4 制定管理政策 7.5 责任 7.6 起诉还是不起诉 7.7 小结第8章 取证(I) 8.1 指导性的原则 8.2 取证硬件 8.3 取证软件 8.4 获取证据 8.5 对证据的检查 8.6 小结第9章 取证(II) 9.1 秘密搜查 9.2 高级搜查 9.3 加密 9.4 家用系统 9.5 UNIX系统和服务器取证 9.6 小结第10章 内部攻击的处理 10.1 内部攻击者的类型 10.2 攻击类型 10.3 对内部攻击的预防 10.4 检测内部攻击 10.5 内部攻击的响应 10.6 特殊考虑 10.7 特殊情况 10.8 法律问题 10.9 小结第11章 事件响应中人性的因素 11.1 社会科学和事件响应的结合 11.2 第一节：计算机犯罪特征描述 11.3 第二节：内部攻击 11.4 第三节：事件的受害者 11.5 第四节：事件响应中人性的因素 11.6 小结第12章 陷阱及伪装手段 12.1 关于陷阱和伪装手段 12.2 陷阱与伪装手段的利与弊 12.3 焦点：“蜜罐” 12.4 事件响应中陷阱和欺骗手段的整合 12.5 小结第13章 事件响应的未来发展方向 13.1 技术进展 13.2 社会进展 13.3 职业发展 13.4 事件的种类 13.5 小结附录A RFC—2196 站点安全手册 A.1 简介 A.2 安全政策 A.3 体系结构 A.4 安全服务和程序 A.5 安全事件处理 A.6 正在进行的活动 A.7 工具和存放地点 A.8 邮件列表和其他资源 A.9 参考资料附录B 事件响应与报告项目检查表

<<网络安全事件响应>>

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>