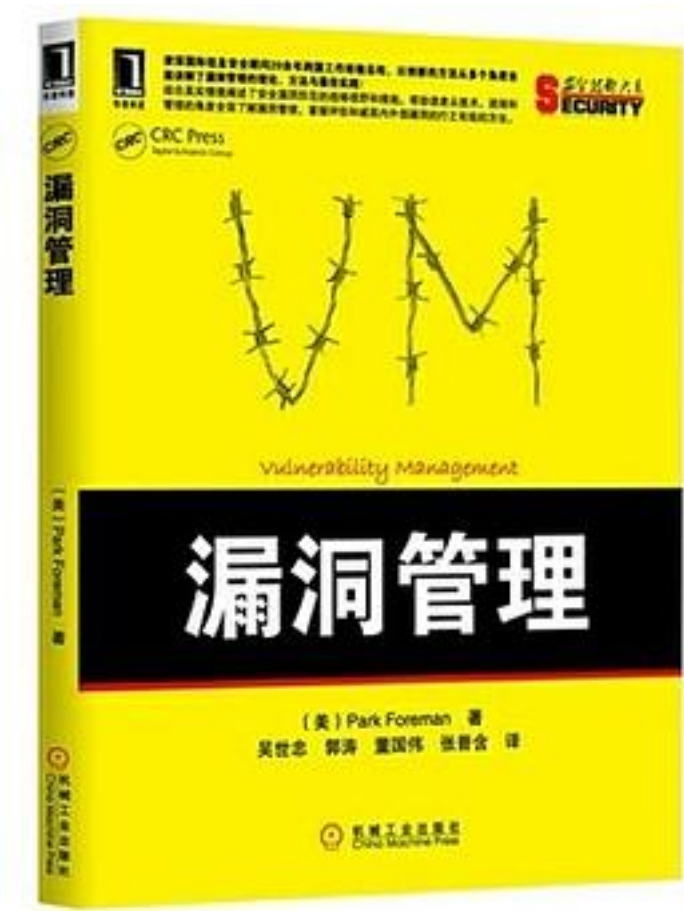


# 漏洞管理



[漏洞管理\\_下载链接1](#)

著者:Park Foreman

出版者:机械工业出版社华章公司

出版时间:2012-12-1

装帧:平装

isbn:9787111401377

本书是资深安全漏洞管理专家、信息安全战略专家兼国际安全顾问20余年跨国工作经验的总结，以创新的方法从多个角度全面讲解了漏洞管理的理论、方法与最佳实践！结合大量实际案例深入阐述了安全漏洞防范的战略视野和实施方式，旨在帮助读者从技术、

流程和管理角度全面了解漏洞管理，从而掌握评估和减弱内外部漏洞的行之有效的方法。

本书共分10章：第1章介绍了风险管理、漏洞管理、安全产业现状等；第2章讲解漏洞产生过程、漏洞程序的作用，并结合实际案例讲解漏洞管理程序故障问题；第3章讲解漏洞管理计划的参与者、漏洞管理策略及合规性；第4章侧重于漏洞扫描的总体架构，并涵盖当前流行的漏洞管理技术，以及漏洞测试相关的数据、评价、技术标准和漏洞管理扫描程序Nessus；第5章阐述了如何选择漏洞管理产品，包括总体要求、实施过程的自动化、体系结构、如何进行用户定制与整合、评分和部署方法、访问控制等相关技术；第6章讲解漏洞管理流程，包括与漏洞管理相关的ITIL-ITSM过程和IAVA过程，以及该流程中的数据分级和风险评估等重要步骤；第7章介绍了一系列与执行、汇报、分析相关的文档，如发现报告、审计报告、合规性报告等；第8章提供了一些建议，引导读者从制定检查表、工程规划和实施策略等方面逐步了解如何在一个大型的公司里开发一个完整的漏洞管理项目；第9章从一个更宏观的、策略性的层面来研究漏洞的呈现形式及修复方法；第10章对上述内容进行了概括性总结。

作者介绍:

Park Foreman

资深漏洞管理专家和信息安全战略专家，资深国际安全顾问，群邑（GroupM）集团的全球信息安全主管，在信息技术领域工作20余年，经验十分丰富。作为一名安全技术顾问，他帮助金融和电信行业的多家公司实现了各种安全目标，并为财富100强企业设计、实施和管理其安全架构。他曾负责贝尔实验室相关应用系统的应用程序开发工作，还曾为世界上最大的几个安全运营中心工作，包括AT&T公司的卓越安全中心（Security Center of Excellence）。此外，他还是一名技术作家，在全球顶级专业期刊（如《Internet Protect》、《ISSA Journal》等杂志）上发表过多篇文章，是全球多个安全组织中信息安全主题和论文的作者。

目录: 译者序

前言

第1章 绪论/1

1.1 风险管理的作用/2

1.2 漏洞管理的起源/3

1.3 安全产业及其缺陷介绍/4

1.4 来自政府和产业的挑战/5

1.5 漏洞的来源/5

1.6 有缺陷的漏洞管理示例/5

1.7 漏洞管理的重要性/6

第2章 漏洞体验/7

2.1 简介/8

2.2 漏洞产生过程/8

2.2.1 复杂性/9

2.2.2 连通性/10

2.2.3 互操作性/10

2.3 创建漏洞：一个例子/11

2.4 使用漏洞管理程序的理由/13

2.4.1 网络过度开放/13

2.4.2 安全系统配置标准缺失/14

2.4.3 重大经济损失风险/14

2.4.4 收益损失/15

2.4.5 生产力损失/15	15
2.5 漏洞管理程序故障/16	16
2.5.1 案例研究1：获得组织的支持 /16	16
2.5.2 案例研究2：技术集成的挑战/22	22
第3章 计划和组织/33	33
3.1 概述：计划结构/34	34
3.2 漏洞管理计划和技术开发/36	36
3.3 参与者/37	37
3.3.1 操作者角色/37	37
3.3.2 贡献者角色/39	39
3.4 策略和信息流/40	40
3.4.1 现行策略/40	40
3.4.2 新策略/41	41
3.4.3 合规和统辖/42	42
3.5 小结/44	44
第4章 漏洞管理技术/45	45
4.1 简介/46	46
4.2 总体架构/47	47
4.2.1 硬件模式/47	47
4.2.2 用户提供的硬件和虚拟化/49	49
4.3 代理/50	50
4.3.1 代理架构/50	50
4.3.2 优点与缺点/52	52
4.3.3 检测方法/53	53
4.4 被动网络分析/53	53
4.4.1 优点与缺点/56	56
4.4.2 检测方法/57	57
4.4.3 物理层/57	57
4.4.4 数据链路层/58	58
4.4.5 网络层/58	58
4.4.6 4至7层/58	58
4.5 主动扫描技术/58	58
4.5.1 优点与缺点/59	59
4.5.2 检测方法/59	59
4.6 混合方法/82	82
4.7 推理扫描/83	83
4.8 CVE/83	83
4.8.1 结构/84	84
4.8.2 CVE的局限/86	86
4.9 漏洞测试数据标准/86	86
4.9.1 架构定义/87	87
4.9.2 系统特征架构/88	88
4.9.3 结果架构/88	88
4.9.4 测试描述/88	88
4.10 漏洞危害程度评价标准 /92	92
4.11 美国国家漏洞库 /98	98
4.11.1 CPE /98	98
4.11.2 XCCDF/100	100
4.12 SCAP/101	101
4.13 Nessus/102	102
4.13.1 优点与缺点/103	103
4.13.2 扫描模型/103	103
4.13.3 使用Nessus/104	104
第5章 选择技术/107	107

5.1 概述/108	
5.2 总体需求/108	
5.2.1 责任分担/108	
5.2.2 时间表/110	
5.2.3 标准/112	
5.2.4 报告/113	
5.2.5 高级报告/115	
5.3 自动化/116	
5.3.1 标签生成/116	
5.3.2 流程整合/117	
5.3.3 流程和系统的灵活性/117	
5.3.4 补丁管理支持/118	
5.4 体系结构/118	
5.4.1 被动的体系结构/119	
5.4.2 基于代理的体系结构/119	
5.4.3 主动扫描的体系结构/120	
5.4.4 保证平台安全/124	
5.4.5 系统整合/125	
5.5 定制与整合/126	
5.6 评分方法/127	
5.7 访问控制/129	
5.7.1 活动目录/129	
5.7.2 RADIUS和TACACS+/130	
5.7.3 授权/130	
5.8 部署方法/131	
5.8.1 主动扫描器部署：物理部署/132	
5.8.2 虚拟扫描器/133	
5.8.3 被动分析器的部署/133	
5.8.4 代理部署/134	
5.9 小结/135	
第6章 过程/137	
6.1 介绍/138	
6.2 漏洞管理过程/138	
6.2.1 准备/139	
6.2.2 发现/140	
6.2.3 轮廓/140	
6.2.4 审计/141	
6.2.5 修复/141	
6.2.6 监控和调整/141	
6.2.7 管理/142	
6.3 基准/142	
6.4 ITIL-ITSM流程/144	
6.4.1 服务支持/144	
6.4.2 服务台/146	
6.4.3 事件管理/146	
6.4.4 服务交付/148	
6.4.5 其他方面/149	
6.5 IAVA流程/149	
6.6 数据分级/152	
6.6.1 案例研究：Big Tyre Corporation/153	
6.6.2 数据分级流程/154	
6.7 风险评估/154	
6.7.1 信息收集/155	
6.7.2 安全控制评估/156	

6.7.3 业务需求/157
6.7.4 资产估值/158
6.7.5 漏洞评估/159
6.7.6 安全控制措施有效性评估/160
6.8 小结/160
第7章 执行、汇报与分析/161
7.1 介绍 /162
7.2 发现报告/162
7.3 评估报告/165
7.4 框架报告/168
7.5 审计报告/171
7.5.1 主动扫描审计报告/171
7.5.2 被动扫描审计报告/172
7.5.3 审计趋势分析/174
7.6 主动扫描：时间安排与资源/177
7.6.1 审计参数/177
7.6.2 时间安排/180
7.7 审计趋势与性能报告/180
7.7.1 基本报告/180
7.7.2 高级报告：控制图/184
7.7.3 介绍漏洞群：控制性能报告/187
7.8 合规性报告/190
7.8.1 系统合规性报告/190
7.8.2 合规性执行总结/192
7.9 小结/193
第8章 规划/195
8.1 介绍/196
8.2 章程制定/197
8.2.1 介绍：业务价值/197
8.2.2 目的和目标/197
8.2.3 范围/198
8.2.4 假设/198
8.3 业务用例/199
8.4 需求文档/199
8.5 安全架构建议/201
8.6 RFP/202
8.7 实施计划/202
8.8 操作流程文档/204
8.9 资产估价指南/205
8.10 漏洞管理策略/205
8.11 部署策略/206
8.11.1 基本策略/206
8.11.2 基于风险的策略/207
8.11.3 改进的时间表/208
8.12 部署标准与进展报告/209
8.13 小结/209
第9章 策略性漏洞/211
9.1 介绍/212
9.2 操作环境/215
9.3 管理外部因素/216
9.4 控制内部漏洞/217
9.4.1 业务模式/218
9.4.2 业务程序/218
9.4.3 复杂性/219

- 9.4.4 反应方案/219
- 9.4.5 漏洞方法论与变更/220
- 9.4.6 复杂性/222
- 9.5 规避原则/223
- 9.6 了解对手/225
  - 9.6.1 优点与缺点/225
  - 9.6.2 现实事件/226
  - 9.6.3 目的与目标的对比/227
  - 9.6.4 时间放大效应/228
  - 9.6.5 政治环境加剧攻击/229
- 9.7 小结/229
- 第10章 总结/231
  - 10.1 介绍/232
  - 10.2 跨领域机会/233
  - 10.3 跨技术机会/234
    - 10.3.1 代理/234
    - 10.3.2 补丁管理/235
    - 10.3.3 应用渗透测试/235
  - 10.4 流程缺陷/236
  - 10.5 运行环境的变化/238
    - 10.5.1 省时/238
    - 10.5.2 节电/238
    - 10.5.3 分布式计算/239
  - 10.6 报告/241
  - 10.7 服务水平协议/241
  - 10.8 小结/241
  - • • • • (收起)

[漏洞管理 下载链接1](#)

## 标签

安全

信息安全

编程

系统攻防

挖漏洞

技术类

## 评论

了解一下漏扫基本概念，漏洞管理流程还是不错的。

-----  
[漏洞管理\\_下载链接1](#)

## 书评

-----  
[漏洞管理\\_下载链接1](#)