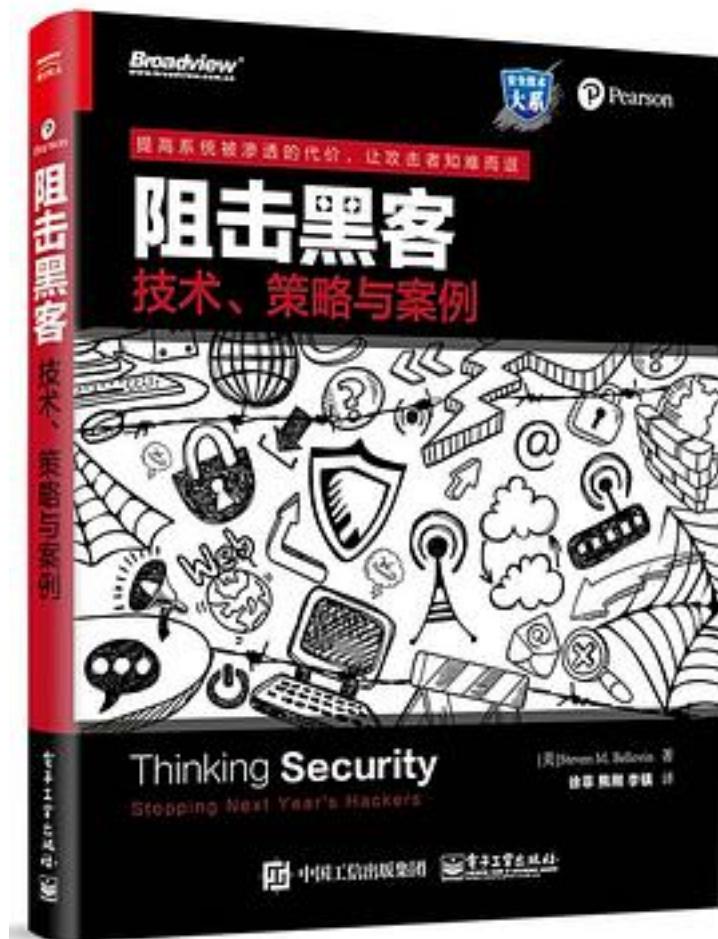


阻击黑客：技术、策略与案例



[阻击黑客：技术、策略与案例_下载链接1](#)

著者: 【美】 Steven M. Bellovin

出版者:电子工业出版社

出版时间:2017-3

装帧:平装

isbn:9787121310669

作者是世界上最受尊重和认可的安全专家之一，它在《阻击黑客：技术、策略与案例》中提供了一种看安全的新视角。

《阻击黑客：技术、策略与案例》第1部分从问题定义开始，从系统化的角度看待安全，讨论当前安全发展的变化、安全的思维方式、目标，并且分析了不同的威胁模型。在此基础之上，第2部分介绍安全相关的技术，除了对技术本身进行介绍之外，作者还很好地考虑了不同情况、不同需求，以及在应对不同威胁模型时，各种技术的优势和可能面临的问题。第3部分介绍具体的安全操作，如何创建安全的系统，考虑了包括代码、设计、架构、管理以及人员等综合因素。第4部分分析具体案例，并且对未来的技术发展和应对给出了建议。

《阻击黑客：技术、策略与案例》基于作者在安全领域多年实际经验，结合新技术的发展，给出了最实用、最综合的安全技术指导，能够为创建安全系统提供很好的借鉴。

作者介绍：

目录: 第一部分 问题定义

第1章 介绍 3

1.1 变化 3

1.2 适应变化 5

1.3 安全分析 8

1.4 用词的一点说明 11

第2章 对安全的思考 13

2.1 安全的思维方式 13

2.2 明确你的目标 14

2.3 安全作为一个系统问题 18

2.4 像对手一样思考 21

第3章 威胁模型 27

3.1 谁是你的敌人？ 27

3.2 攻击的分类 30

3.3 高级可持续性威胁（APT） 31

3.4 什么处在威胁之中？ 35

3.5 期限问题 36

第二部分 技术

第4章 防病毒软件 39

4.1 特征 39

4.2 防病毒软件的养护和培育 44

4.3 随时都需要防病毒吗？ 46

4.4 分析 49

第5章 防火墙和入侵检测系统 53

5.1 防火墙不做的事 53

5.2 防火墙的原理 54

5.3 入侵检测系统 60

5.4 入侵防御系统 61

5.5 泄露检测 62

5.6 分析 66

第6章 加密和VPN 69

6.1 加密——特效药 69

6.2 密钥分发 72

6.3 传输层加密 73

6.4 客体加密 75

6.5 VPNs 79

6.6 协议、算法和密钥长度建议 82

6.7 分析 89

第7章 密码和认证 93

7.1 认证的原则	93
7.2 密码	93
7.3 存储密码：用户	99
7.4 密码被盗	103
7.5 忘记密码	105
7.6 生物特征	107
7.7 一次性密码	111
7.8 加密认证	115
7.9 令牌和手机	116
7.10 单点登录和联合认证	119
7.11 存储密码：服务器	121
7.12 分析	124
第8章 PKI：公钥基础设施	129
8.1 什么是一个证书？	129
8.2 PKI：你相信谁？	130
8.3 PKI与pki	134
8.4 证书的过期和撤销	139
8.5 分析	144
第9章 无线访问	147
9.1 无线不安全的迷思	147
9.2 保持连接	153
9.3 断开连接	155
9.4 智能电话、平板、玩具以及移动电话接入	156
9.5 分析	157
第10章 云和虚拟化	161
10.1 分布式和隔离	161
10.2 虚拟机	162
10.3 沙箱	164
10.4 云	167
10.5 云提供商的安全架构	168
10.6 云计算	169
10.7 云存储	170
10.8 分析	172
第三部分 安全操作	
第11章 创建安全系统	179
11.1 正确的编码	180
11.2 设计问题	183
11.3 外部链接	186
11.4 可信方	189
11.5 原始系统	192
11.6 结构化防御	194
11.7 安全评估	196
第12章 选择软件	201
12.1 质量问题	201
12.2 明智地选择软件	204
第13章 及时更新软件	209
13.1 漏洞和补丁	209
13.2 补丁的问题	211
13.3 如何打补丁	213
第14章 人的因素	215
14.1 雇员、培训和教育	215
14.2 用户	218
14.3 社会工程	220
14.4 可用性	222

14.5 人的因素	228
第15章 系统管理	231
15.1 系统管理员：你最重要的安全资源	231
15.2 走正确的路	233
15.3 系统管理工具和架构	235
15.4 将系统管理外包	238
15.5 黑暗面是权力	239
第16章 安全过程	241
16.1 计划	241
16.2 安全策略	242
16.3 记录和报告	245
16.4 事件响应	248
第四部分 关于未来	
第17章 案例分析	253
17.1 小型的医疗实践	253
17.2 电子商务网站	255
17.3 加密的弱点	257
17.4 物联网	259
第18章 恰当的做法	267
18.1 过时	267
18.2 新设备	268
18.3 新的挑战	269
18.4 新的防御	270
18.5 考虑隐私	271
18.6 整体考虑	271
参考文献	273
版本信息	325
• • • • •	(收起)

[阻击黑客：技术、策略与案例](#) [下载链接1](#)

标签

黑客

评论

感觉这本书一般，都是泛泛而谈，纯科普读物！初学者看不懂，经验者看完无感！

[阻击黑客：技术、策略与案例](#) [下载链接1](#)

书评

相对于cissp, cisa, cism培训内容的条款和技术规则的枯燥，这本书尽量用IT领域的通用语言，经验，技巧和案例，阐述自己CISO的经验以及具备学术领域验证的观点，从严肃性的角度出发，长达52页的引文可见一斑，作为美国联邦贸易委员会cto的belovin，其权威性应该也毋庸置疑...

[阻击黑客：技术、策略与案例 下载链接1](#)