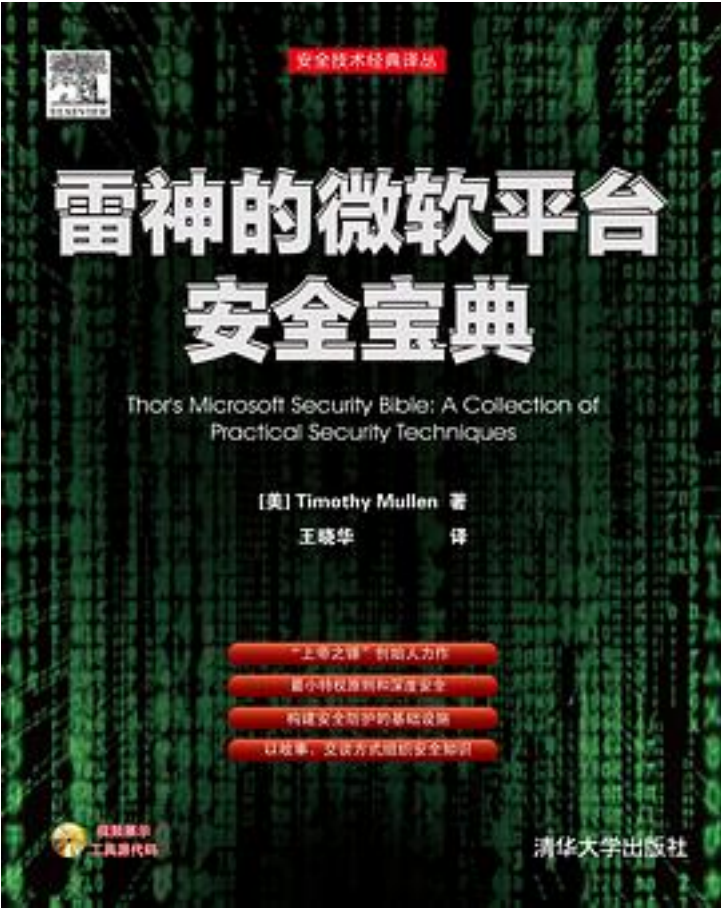


雷神的微软平台安全宝典



[雷神的微软平台安全宝典_下载链接1](#)

著者:(美)马伦(Mullen, T.) 著

出版者:清华大学出版社

出版时间:2013-1

装帧:

isbn:9787302307433

以最有效、最便捷的方式构建安全防护的基础设施

《雷神的微软平台安全宝典》为读者学习微软平台相关的安全技术提供了“一站式”解决方案，这些技术可以用于部署一些典型的基础安全设施。本书从多个层面详细描述了

安全相关的概念和方法论，包括服务器、客户端、组织结构、特定平台相关的安全选项、应用程序相关的安全特性(IIS、SQL、活动目录等)，还包括一些新的、从来没有发布过的安全工具，这些安全工具都带有完整的源代码。

主要内容

- 针对所有主流的微软应用程序的安全过程提供了详实的技术信息



采用独特的、基于项目的“讲故事”表达方式，同时组合多种安全技术和方法以应对现实世界中实际商业模式面临的安全挑战

- 内容的组织方式使得访问特定应用程序的安全技术和方法变得易如反掌



采用独特的观点和视角，使读者对解决特定应用程序安全方案的方法不仅“知其然”，而且“知其所以然”

- 随书发布的DVD光盘包含了源代码、工具、视频教程以及其他有用的资料

作者介绍:

Timothy

Mullen是某个价值数十亿美元的商务平台的首席安全架构师，该商务平台在全球范围内被广泛应用。Timothy被称为“雷神”，也是“上帝之锤”安全合作组织的创始人。他是美国门萨俱乐部的成员、微软的认证讲师。对于微软新发布的每一款操作系统，他都通过了微软工程师认证，在Windows企业安全领域连续4年被授予MVP称号。

目录: 目录

第1章 将Web代理日志安全地写入SQL Server数据库中，并通过编程监视Web数据流量，自动向TMG添加“允许/拒绝”规则 1

1.1 引言 2

1.2 范围和关注的事情 3

1.3 实现 5

1.3.1 将权限委托给用户 6

1.3.2 TMG访问规则 8

1.4 安全地将日志写入SQL Server数据库中 9

1.4.1 在SQL Server中创建TMG服务器用户账户 11

1.4.2 配置登录选项 12

1.4.3 测试连接 13

1.4.4 保证SQL通信通道的安全 14

1.4.5 证书登记和配置 15

1.4.6 TMG特别登记 16

1.4.7 故障排除 18

1.4.8 测试和验证 20

1.5 设计工作流 21

1.6 执行 24

1.6.1 xp_cmdshell 25

1.6.2 CmdExec 25

1.6.3 SQL CLR 30

1.6.4 可选方案 35

1.6.5 利用AppLocker 39

1.7 本章小结	40
第2章 IIS认证和授权模型，使用EFS和WebDAV锁定文件访问	41
2.1 引言	42
2.2 RSA和AES	44
2.2.1 EFS规划和故障解决	48
2.2.2 事后用例分析	51
2.3 构建Web应用程序结构	52
2.3.1 访问概述	52
2.3.2 应用程序池	56
2.4 访问远程文件	59
2.4.1 虚拟目录	59
2.4.2 服务用户	63
2.5 深度安全	66
2.5.1 使用EFS	67
2.5.2 EFS和服务用户	67
2.5.3 为共享文件建立EFS	68
2.5.4 委托	70
2.5.5 检查点	76
2.6 使用WebDAV提供安全访问	77
2.6.1 安装WebDAV	77
2.6.2 配置WebDAV	78
2.6.3 映射远程WebDAV驱动器的好处	79
2.6.4 WebDAV和EFS——没有委托	80
2.6.5 WebDAV和EFS——数据移动	80
2.7 结论	81
2.8 本章小结	82
第3章 根据地理位置分析和阻止恶意流量	83
3.1 引言	84
3.2 研究和尽职调查	84
3.3 实现一种解决方案	86
3.3.1 记录流量	88
3.3.2 数据函数	89
3.3.3 建立数据之间的联系	93
3.3.4 处理流量来源国家	95
3.4 与TMG集成	96
3.4.1 决策，再次决策……	97
3.4.2 保持简洁	100
3.4.3 引入SQL CLR	103
3.4.4 构建ISA服务器/TMG计算机集	108
3.5 本章小结	116
第4章 以安全的方式创建可以从外部访问的认证代理	117
4.1 引言	118
4.2 做好准备，该来的自然会来	118
4.2.1 认证挑战	120
4.2.2 认证机制	123
4.2.3 发布代理	124
4.3 本章小结	133
第5章 创建和维护低特权服务用户	135
5.1 引言	136
5.2 创建并配置服务用户账户	137
5.2.1 活动目录的结构	138
5.2.2 准备应用程序	141
5.2.3 组策略对象配置的设置示例	146
5.3 真实、可量化的密码强度以及如何衡量密码强度	155

5.3.1 一种新方法	156
5.3.2 字典攻击和其他攻击方法	160
5.3.3 查看代码	161
5.4 本章小结	165
第6章 在最小特权环境中收集远程安全日志	167
6.1 引言	168
6.2 日志提取程序的架构	169
6.2.1 检索日志数据	169
6.2.2 日志文件访问和权限	179
6.2.3 自定义Windows日志权限	181
6.3 访问WMI对象	197
6.3.1 构建WMI组件	197
6.3.2 加密DCOM WMI连接	200
6.3.3 其他WMI示例	203
6.4 查看代码	207
6.4.1 SQL Server的数据结构	208
6.4.2 向SQL Server发送数据	209
6.4.3 日志提取程序代码总结	217
6.5 本章小结	218
第7章 确保远程桌面协议的安全	219
7.1 引言	219
7.2 常见的RDP攻击和防范	221
7.2.1 重命名管理员账户并使用强壮的密码	222
7.2.2 RDP服务端口	222
7.2.3 网络级别身份验证	224
7.3 RDP解决方案概述	225
7.4 直接访问多台RDP主机	226
7.5 RDG/TSG	227
7.6 RDP主机的安全性	231
7.7 RDWeb和RemoteApp	233
7.7.1 RDWeb	234
7.7.2 RemoteApp	235
7.7.3 部署经过签名的RDP文件	238
7.7.4 RemoteApp和桌面连接(WebFeed)	242
7.8 工作站主机的注意事项	243
7.9 使用源端口访问规则来限制访问	245
7.10 查看代码	249
7.11 本章小结	257
附录A 首字母缩略词列表	259
附录B 利用WEVTUTIL工具从Windows Server 2008获取的完整日志列表	263
• • • • •	(收起)

[雷神的微软平台安全宝典 下载链接1](#)

标签

计算机安全

安全

评论

[雷神的微软平台安全宝典_下载链接1](#)

书评

[雷神的微软平台安全宝典_下载链接1](#)