安全技术经典译丛

雷神的微软平台安全宝典

Thor's Microsoft Security Bible: A Collection of Practical Security Techniques

[美] Timothy Mullen 著

王晓华 译

“上帝之锤”创始人力作

最小特权原则和深度安全

构建安全防护的基础设施

以故事、交谈方式组织安全知识

视频展示
工具源代码

清华大学出版社

安全技术经典译丛

雷神的微软平台安全宝典

[美] Timothy Mullen 著

王晓华 译

清华大学出版社

北 京

Thor's Microsoft Security Bible: A Collection of Practical Security Techniques
Timothy Mullen
EISBN：978-1-59749-572-1
Copyright © 2011 by Elsevier. All Rights Reserved.

Authorized Simplified Chinese translation edition published by the Proprietor.
Copyright © 2011 by Elsevier (Singapore) Pte Ltd. All rights reserved.
Published in China by Tsinghua University Press under special arrangement with Elsevier (Singapore) Pte Ltd.. This edition is authorized for sale in China only, excluding Hong Kong SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由 Elsevier (Singapore) Pte Ltd.授予清华大学出版社在中国大陆地区(不包括香港、澳门特别行政区以及台湾地区)出版与发行。未经许可之出口，视为违反著作权法，将受法律之制裁。
北京市版权局著作权合同登记号：01-2012-2720

本书封面贴有 Elsevier 防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

雷神的微软平台安全宝典 /(美)马伦(Mullen, T.) 著；王晓华 译. —北京：清华大学出版社，2013.1
(安全技术经典译丛)
书名原文：Thor's Microsoft Security Bible: A Collection of Practical Security Techniques
ISBN 978-7-302-30743-3

Ⅰ. ①雷… Ⅱ. ①马… ②王… 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(2012)第 284166 号

责任编辑：王　军　李维杰
装帧设计：牛艳敏
责任校对：邱晓玉
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　印　　张：18　　字　　数：352 千字
(附光盘 1 张)
版　　次：2013 年 1 月第 1 版　　印　　次：2013 年 1 月第1 次印刷
印　　数：1～3000
定　　价：58.00 元

产品编号：045275-01

作者简介

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。

技术编辑简介

Jeffrey W. Brown(CISSP-ISSMP、CISM、CRISC、PMP)是资深的信息安全专家，拥有 14 年为世界财富 500 强公司制定、实施企业安全规划的经验，他制定的安全规划可以满足这些公司在业务、监管以及信息安全等各个方面的需求。Jeffrey 现在是通用电器金融财务公司的全球信息安全项目经理，负责全球信息安全和 IT 风险活动的开发与实施。他拥有丰富的行业经验，是多个行业协会的咨询委员会的成员或参与者，包括 ISSA、ISACA 和 The Technology Manager 论坛，他还是纽约 CISO 执行首脑峰会的管理成员。Jeffrey 曾是 SANS *Windows Security Digest* 编辑委员会的成员，参与编辑过几部 SANS Step-by-Step 系列指导丛书，包括 *Windows NT Security Step-by-Step*、*Windows 2000 Step-by-Step* 等。Jeffrey 拥有美国佩斯大学的学士学位和硕士学位，还曾是一些出版物的作者和撰稿人，比如 *Mission Critical Internet Security* 等。

此为试读，需要完整PDF请访问：www.ertongbook.com

前言

什么是安全？是一种思维方式吗？还是一种可衡量的、可操作的看法或态度？抑或与两者都有一点关系？人类，作为一个种族，根据以前学到的知识构建新的知识已经成为我们内心根深蒂固的过程，正如牛顿说的那样：“如果我看的比别人远，那是因为我站在巨人的肩膀上。”从根本上讲，当我们处理新的信息时，可以把旧的信息当作基础。

但这对我们并不总是有用，特别是在技术领域，技术总是以自身特有的方式暴露我们以过去思维方式填补人们之间假设的空白时产生的缺陷。技术可以回答很多问题，但是坦白地说，这些问题都是以前被某些人即兴回答过的问题。笔者认为科学和宗教之间的关系也是很好的例子，随着技术的进步，越来越多关于这个世界的事情被解开了神秘的面纱，这些事情以前都被解释为神的意志或是魔法。那些给出这些答案的人被尊为某种方法的大师，被抬到受人尊敬的神坛上膜拜，他们中的一些人的确是天才，乐于用他们的洞察力和智慧帮助其他人，而另一些人则是一群冒牌的“大师”，他们怀有私心，编造一些既不明智又缺乏洞察力的故事，他们甚至可能就是一群“蛇油推销员”。笔者的目的不是预言什么事情，而是提出建议，这些建议能帮助大家清楚地分辨出哪些是对保持信息安全有价值的历史教训，哪些是一堆毫无意义的废话。

安全策略需要规划和事件响应，就像在滑动的鳞片上移动目标那样。载体和目标都会随着技术的变化而变化，或随着罪犯收入来源的枯竭而变化。新的目标不断被物色出来，在家用环境中针对用户的攻击和行为模式将会迁移到移动领域，无论是个人还是商务应用，越来越多的业务都将会用手机完成。但是随着攻击目标的变化，仍然保持不变的还是构建安全防护的基础设施，这些基础设施应该就是深度安全和最小特权原则。之所以这么认为，是因为到目前为止这方面的话题讨论已经有十几年时间了，这两个安全概念依然和当初一样值得信赖。

现在的安全行业正在被引导至错误的方向，实际上已经违反了最初存在的目的，离实际的信息安全越来越远，反而更像是三环马戏团的营销手段。如今，安全看起来全是黑客们的自我炫耀。如果参加过任何流行的安全大会，就会发现会议的主题实际上已经不是有关安全的了，更像是反安全的：如何黑掉这个、如何攻击那个、如何入侵什么等等。随着时间的推移，攻击方法变得更精密，更复杂，即使那些很少可能发生的攻击现在也变成日常的威胁。参会的演讲者看起来不是展示如何更安全，而是炫耀自己如何优秀。如果能提出一些疯狂的方法做一些独特的事情，他就会认为是天才，对他展示的东西你就得照单全收。

研究者找到 bug 并对外公布，只是想借此提高他们的知名度，而不是像他们经常宣称的那样：促使软件公司提高软件的安全性。他们希望自己发现的问题越严重越好，总是试图发现最糟糕的情况是什么。他们往往忽略那些最简单的逻辑点，如设置一下载体的权限就可以防止被利用之类的方法。更重要的是，那些打着安全建议旗号出售的东西往往十分的蹩脚，一些非常不起眼的安全问题被夸大其词为危险的安全漏洞。有人可能会说，正是这种级别的公开监督才使得整个产业越来越安全，这样做也无可厚非。但是，随着这样的“蛇油推销员”越来越多，真正有志于信息安全的聪明人士反而越来越少。

说句公道话，笔者确实看过一些真正有趣的，甚至是非常吸引人的攻击系统的方法，都是一些非常聪明的方法，但是要在现实世界的业务中应用还不太可能。如果用刚才那个马戏团的比喻，就像杂技演员互相头顶头倒立翻转，降落时一只脚落在另一个人的手上，这真的相当了不起，需要大量的练习和技巧，但是却没有做任何真正的事情。虽然，这是艺术并且有娱乐的价值，但是从生产的角度看，这些人没有创造任何东西，差不多可以说，这些都是表演。

这也就是本书为什么总是从防守的角度展示信息安全问题的原因所在，本书指导的每一次练习以及展示的每个示例都是基于如下思想：这样做可以保护你不受某种攻击。对你来说，这就是价值所在，花 5 分钟时间展示给大家的一些设置方法，可以防止那些需要花 5 个小时时间黑客训练才能学会的攻击手段的攻击，这应该是更理所当然的一种做事的方法。

于是，这听起来可能有点可笑，没有被黑过反而很无聊。攻击失败之后再来观看失败的攻击过程并不十分有趣，这也是为什么没人卖安全的原因。观看杂技演员的表演和打开一扇门一样安全，然而觉得钱花得值是因为表演能吸引我们的注意力。这本书介绍的是如何构建安全基础障碍以提高系统的安全态势，如何在最小特权环境中部署符合深度安全的解决方案，如何使用现有的系统获得更好的安全态势而不是继续花钱买新的安全产品。希望这本书有别于那些只关注某一种应用观点的安全书籍，同时

希望本书展示的资料有别于那些典型的以学院派方式编写的书籍，这本书做到了这两点。这本书是以交谈的方式组织的，基本上就是观点和方法的集合，这些观点和方法都是笔者过去在安全领域积累的独特方法，它们以非常自然的方式传授给你，就好像我们互相面对面坐在一起交谈一样。为了让各种安全观点都能够被接受，本书模拟创建了各种业务场景问题，然后找出相应的解决方案，这些都和现实世界中实际的工作情况相一致。例如，不仅仅是保证 SQL Server 安全，通过阅读本书，实践其中的例子，最终可以保证所有围绕着 SQL Server 构建的过程都是安全的。所以在这些故事中，情节就是在我们曾经经历过的商业项目中，将各种不同性质的产品和产品特征结合在一起完成工作。

这些故事不仅仅是关于业务场景的，和其他的宝典书籍一样，每个故事都是一段教学课程，了解这一点很重要。当读到关于如何写一段特殊的代码或以某种特殊的方式创建用户以完成某些特定的事情时，希望你能思考一下如何将同样的概念应用到其他事情上。通过这些例子，你会看到本书接下来要介绍的场景，在这个场景中你会了解到如何将防火墙代理日志数据记入 SQL Server，如何将 SQL Server 运行在低权限用户的上下文中，如何为保证数据一致性而加密所有网络连接过程。虽然项目可能会创建自主日志监视以便自动实施访问规则，但还是可以使用完全相同的处理来保证其他应用程序在向 SQL Server 记录日志时的传输数据也是加密的。换句话说，每个故事都蕴含着一些超越故事本身的东西。

说到这里，我们还要介绍一下本书其他有用的内容。除了每章的文字内容之外，在随书光盘中还有贯穿本书内容的视频展示和示例代码，这些附加内容涵盖了更宽范围的主题、观点和处理方法。笔者将演示如何像前面提到的那样创建自主流量监控，如何根据国家和国家的地理位置汇编和报告流量，如何建立安全的外部 Web 代理，如何保证远程桌面协议的安全，如何使用最低权限并以安全的方式建立远程安全日志系统，以及如何为维护服务使用者提供相关的诀窍、计谋和更多的内容。

本书尝试以循序渐进的方式介绍每个故事或项目，尽量与你自己冒险创建项目时要做的过程一致。也就是说，当你尝试亲自解决某个问题的时候，笔者会模仿你可能收获的经验。笔者喜欢用系统的方法解决项目问题，因为多次重复项目的某个特定方面不可能使你真正了解它，除非亲自遇到。当然，笔者对人生、宇宙和其他事物的一些看法也交织在其中。所以，感谢你购买这本书支持“上帝之锤”的研究成果。事不宜迟，现在就开始吧。

目录

此为试读，需要完整PDF请访问：www.ertongbook.com

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

本章主要内容包括

- 实现
- 将日志数据安全地写入 SQL Server 数据库中
- 设计工作流
- 执行

产品、工具和方法

- 活动目录

- SQL Server 数据库
- 支持高级安全特性的 ISA 服务器/TMG[1]
- 将 TMG 日志写入 SQL Server 数据库中
- 最小特权服务用户
- 使用 SQL 公共语言运行时(CLR)代替 xp-cmdshell
- 活动目录的权限委托
- 组织单位
- TMG 拒绝规则
- 计算机证书
- AppLocker

1.1 引言

下面介绍一个例子，目的是将微软 TMG(Threat Management Gateway)的日志功能和强大的 SQL Server 数据库安全地结合在一起，监视用户的通信流量，侦测用户是否违反了公司(或其他地方)的网页浏览政策。侦测的方法就是检查用户在浏览器的目的地址栏中输入的目的地址 URI(Uniform Resource Identifier)，看看是否和预先设定在黑名单中的网站地址匹配。如果用户访问黑名单中的地址，就会阻止用户继续使用活动目录的组成员关系，这个组成员关系是动态管理的，而且例子中的阻止操作是自动完成的。这个例子中的一些技术都可以被应用到各种不同的场景中，你可以注意一下，看看能否将这些方法移植到其他应用程序和配置中。

在这个例子中，我们将使用集成的机器凭证将 TMG 的 Web 代理日志导入到 SQL Server 数据库中，然后创建 SQL 查询来监视日志中的条目。当满足条件时，就触发一个事件，SQL Server 响应这个事件，将触发这个事件的用户所属的组更换成 AD(Active Directory，活动目录)全局组。因为这个全局组已经被 TMG 预先设定了拒绝规则，所以用户会被阻止继续访问网络。

换句话说，SQL 将几乎实时地监视 TMG 日志，检查日志中的目的地址是否匹配管理员预先设定好的黑名单网址。如果有用户违反网页浏览政策(比如上班时间访问 ESPN 网站)，系统就会自动执行命令，将这个用户加入到一个全局组中。在 TMG 中，这个全局组的组成员都被禁止访问外部网络。当规则匹配的时候，除了要显示默认的

1 从现在开始，我们只讨论与 TMG 有关的内容，不过 TMG 的很多选项也可以用在 ISA 服务器中。

TMG 访问错误页面给用户之外，还要将用户的访问重定向到某个内部网页，在那里用户将听到雷神之锤：Quake Arena(一款竞技场游戏)里的 DENIED.wav 声音，同时会看到旋转的骷髅头告诉用户外网访问失败了，快收拾东西去前台报告(译者注：暗指卷铺盖回家，炒鱿鱼)。实际上，我曾经用这种方法在以前工作过的公司部署过真实的生产环境，结果确实令一些人感到惊讶，但是并没有引起太多的抱怨，因为大家都把这当作一件好玩的事情而接受了。当然，对于读者来说，可以自己决定是否采用和我一样的做法。

在实现这个例子的每一步骤中，我都会尽可能地提醒大家，什么样的过程环境适合创建并使用深度安全和最小特权原则。虽然这里介绍的内容都只是一些整合在一起的可用的例子，但是我会保证每个例子都尽可能完整，就像可以直接编译的完整源代码那样，可以直接使用。和那些不值得写在 HTML 里(指在网上发表的文章)的安全理论不一样，我所提出的想法在理论上都是完整的、经过测试的，并且具有可操作性。总之，这些处理方法可以应用到各种不同的安全过程中。

1.2　范围和关注的事情

我曾经见过很多 SQL 环境中的计划任务都是以管理员身份运行的，使用曾经十分流行的 xp_cmdshell 作为命令解释器扩展 SQL Server 的存储过程，因为 xp_cmdshell 可以直接与操作系统(Operating System，OS)或文件系统交互。要是几年前，确实没有太多方法能够比 xp_cmdshell 更可靠地完成这些工作，那时候人们也不像现在这样担心安全性问题。对于类似的问题，过去通常的做法就是将 SQL 设置成混合认证模式，使用数据源名称(Database Source Name，DSN)在 TMG box 中连接 SQL Server，用存储的信用凭证上传日志记录，在拥有特权的用户上下文中运行 SQL Server 服务。这样，这个拥有特权的 SQL Server 服务就可以利用前面提到的 xp_cmdshell 执行类似 net use 这样的命令，进而直接修改活动目录中的组成员关系。

但是采用这种配置方式会造成几个不好的结果，比如可能会在系统中产生漏洞，使得攻击者可以利用漏洞在服务账号的用户上下文中执行恶意代码。也可能会使得 SQL 注入的媒介(载体)允许将攻击者定制的脚本注入 SQL 代码中。如果 xp_cmdshell 被配置为可用状态，那么注入 Transact-SQL(T-SQL)代码，使之启动 Windows 命令行提示窗口并在这个命令行窗口中向管理员组添加用户将易如反掌。有了这个命令行窗口，远程生成 cmd 脚本并执行也是一件很容易的事情。比如，攻击者可以使用 echo ftp > getit.cmd 命令一次一行地在服务器上生成名为 getit.cmd 的 cmd 脚本文件，里面的内容可以是连接到某个 FTP 服务器并下载一些工具的脚本代码，然后只要执行 echo open

>> getit.cmd 就可以在远程服务器上运行这个脚本，下载一些攻击者惯用的工具软件到这个服务器上。从此以后，攻击者就可以在服务器上执行这些工具并做任何事情，比如直接连接到服务器，窃取用户数据等等。由此可见，在 SQL Server 上启用 xp_cmdshell 配置是一件多么危险的事情，尽管现在 SQL 已经默认禁用了 xp_cmdshell，但是不少人还是习惯用这个功能强大的 xp_cmdshell 做一些肮脏的事情。本章的例子不会使用 xp_cmdshell，事实上，我们会用三个例子循序渐进地给出不好的、好的和更好的解决方法并详细讲解最终的优选方案：SQL CLR。

1.2.1 安全进程的前提条件

完成这个练习有两个前提条件。首先，需要 SQL Server 服务以最小特权用户的身份运行，就像第 5 章“创建和维护低特权服务用户”中讨论的那样，按照这一章总结的方法做下来就是：以主域用户 HAMMEROFGOD\SQLUser 的权限运行 MSSQLSERVICE 服务，SQLUser 是 HAMMEROFGOD\gServiceUsers[2]全局组的成员，这个组的用户除了在安装 SQL Server 的时候拥有指定的权限之外，没有任何其他权限。更特殊的地方是，这个用户不属于任何内置的组，因为该用户已经被显式地从默认的主域用户组删除了。系统身份验证使用 Windows 认证(或集成 Windows 认证)方式，因为这种方式可以从 Windows 继承账户锁定和增强的密码复杂性等安全好处，这一点也是第 5 章讨论的方法。

其次，为了使 TMG 在 Web 代理日志中能够正确地记录 Windows 用户的用户名，还需要确保外网访问需要认证。所有的浏览器初始状态都是使用的匿名用户的上下文，即便配置了代理也是如此。如果 TMG 的外网访问的权限规则被配置成允许所有用户访问，那么匿名用户访问外网的请求也会被授权允许访问。最后，日志文件看起来如下所示(截取的数据片段)：

```
ClientIP    ClientUserName   DestHost       DestHostIP
3232235829  anonymous        www.bing.com   3232235786
```

请注意，日志记录的客户端的用户名是 anonymous，因为正如上述配置期望的那样，匿名用户也满足 TMG 规则，所以拥有直接访问外网的权限。还需要注意的是，日志记录的客户端的 IP 地址和目的主机的 IP 地址都是长整型数字，正常情况下，日志就以这种格式记录。第 3 章 “根据地理位置分析和阻止恶意流量”会介绍如何实现标量函数，使用标量函数可以非常容易地将长整型数字转换成 IP 地址的点分十进制格

2 我在每个全局组的名字前都加了前缀 g，这样在排序显示的时候，这些组就可以显示在一起。

式。完成设置后的 TMG 规则应该和图 1-1 显示的配置一样，当然，你也可以设置成基于其他本地组或主域组的认证方式，只要禁止允许所有用户访问的规则，TMG 就会强制要求每个用户进行认证。

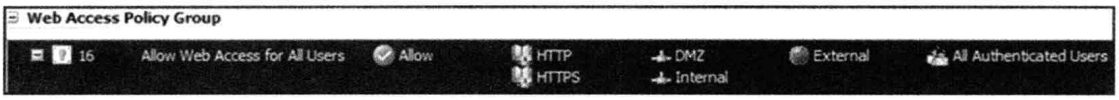

图 1-1　TMG 访问规则显示的每个认证用户使用 HTTPS 访问外网的权限

事实上，前面所做的这些配置并没有改变浏览器的默认行为，知道这一点很重要，例如 Internet Explorer(IE)，一开始仍然会尝试匿名连接，只是 TMG 会拒绝请求并要求(挑战)IE 确认认证凭证。这个要提交给 TMG 的认证凭证可以是集成认证方式，也可以显示凭证登录对话框(这取决于如何配置浏览器和域属性)。现在，系统记录到的日志看起来应该如下所示：

```
ClientIP      ClientUserName        DestHost        DestHostIP
3232235829    anonymous             www.bing.com    3232235786
3232235829    HAMMEROFGOD\thor      www.bing.com    3232235786
```

当生成报告的时候，可以选择自己删除匿名用户的日志记录项，简单地说就是将它们从查询条件中删除，也可以选择在第一时间就排除这些记录。哪种方法最适合你，就用哪种方法。我的做法是删除匿名的请求记录，因为在我的环境中，我只需要所有认证用户的 Web 访问记录，不关心那些匿名尝试。当然，我的日志信息可能不适用于你的环境，或者可能你会发现分析源客户端的信息(比如浏览器类型)很有用，可以帮助你清除网络中的恶意接入尝试，这就要看你自己的配置方式了。

1.3　实现

假如前面提到的前提条件都满足了，就可以继续刚才的处理过程。既然需要根据组成员关系阻止所有的外部访问企图，所以创建目标全局组，目标全局组将作为容器，用于存放那些被拒绝访问的用户。如果要拒绝某个用户访问外网，就把这个用户移到这个组中；如果要恢复某个用户的外网访问权限，就把这个用户从这个组中移走。

还有一件重要的事情需要注意，为了让自主流量分析系统正常工作，SQL Server 的数据库引擎(具体在这个例子中就是 SQL Server 代理)必须亲自执行组成员关系的指

此为试读，需要完整PDF请访问：www.ertongbook.com