ELSEVIER

信息安全丛书

# 信息安全最佳实例

[美] George L. Stefanek 著

吴世忠 李斌 郭涛 译

重庆大学出版社

http://www.cqup.com.cn

# 信息安全最佳实例

George L. Stefanek 著
吴世忠 李 斌 郭 涛 译

重庆大学出版社

**图书在版编目(CIP)数据**

信息安全最佳实例/(美)斯蒂芬克著;吴世忠等译.
重庆:重庆大学出版社,2006.10
(信息安全丛书)
ISBN 7-5624-3649-5

Ⅰ.信... Ⅱ.①斯... ②吴... Ⅲ.信息系统—安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2006)第 044703 号

版贸核渝字(2005)第 46 号

**信息安全最佳实例**
Xinxi Anquan Zuijia Shili
[美]George L. Stefanek 著 吴世忠 李 斌 郭 涛 译

**出 版 者**:重庆大学出版社 **地 址**:重庆市沙坪坝正街 174 号重庆大学(A 区)内
**网 址**:http://www.cqup.com.cn **邮 编**:400030
**电 话**:(023) 65102378 65105781 **传 真**:(023) 65103686 65105565
**出 版 人**:张鸽盛
**责任编辑**:王 斌 戴倩倩 **版式设计**:王 斌
**责任校对**:方 正 **责任印制**:赵 晟
**印 刷 者**:重庆升光电力印务有限公司
**发 行 者**:全国新华书店经销
**开 本**:787×1092 1/16 **印张**:6.75 **字数**:129 千
**版 次**:2006 年 10 月第 1 版 2006 年 10 月第 1 次印刷
**书 号**:ISBN 7-5624-3649-5
**印 数**:1—3 000
**定 价**:18.00 元

# 译者序

当前，信息安全问题日趋严重：间谍软件、计算机病毒、垃圾邮件等恶意软件层出不穷；各种信息系统的可用性时遭破坏；黑客攻击事件，网上银行和网上证券的失泄密事件也频繁发生。造成这些信息安全问题的主要原因之一就是用户缺乏必要的计算机安全知识。

目前市面上虽然已有不少的信息安全书籍，但主要以介绍信息安全基本概念和理论、密码算法、黑客技术的居多，普通读者阅读起来有一定难度，同时也缺乏可操作性和指导作用。

针对上述情况，George L. Stefanek 先生总结了自己在信息安全领域方面可贵的工作经验，编写了《信息安全最佳实例》一书。本书从技术和管理两个方面出发，总结出 205 条网络与信息安全实用指南，内容涵盖了网络管理、信息安全策略制定、信息安全网络体系制定、选择安全的软硬件、物理安全、网络硬件安全、操作系统安全、网络安全、应用程序安全、软件确认和验证、数据加密、配置管理、网络监控、维护和故障检修安全、培训、紧急事件处理等方面的内容，为普通计算机用户、网络管理员和信息安全管理员提供了非常好的安全指导。本书具有很强的实用性和可操作性，合理运用其中的一些知识可以有效地防止常见的黑客攻击，降低网络与系统受攻击的风险。它不仅适合于信息安全科研人员阅读，也可作为信息安全从业人员的参考指南。我们希望本书对所有读者都能有所裨益。

本书由吴世忠、李斌、郭涛主持翻译，其他参与翻译的人员还有张动、李淼、张彬彬、易郡等，宋云生、田惠文、向继志等同志在文字校对上也付出了辛勤的劳动，在此一并表示感谢。

由于水平所限，不妥或错误之处在所难免，敬请广大读者批评指正。

译　者

2006 年 5 月

于中国信息安全产品测评认证中心

# 前　言

本书的目的是向初学者和系统管理员提供一套实用的规则或者“最佳实例”，如果读者在具体过程中遵照这套规则执行，就可以保障其组织的信息安全(INFOSEC)。本书中的这些实例均来自于作者多年的实践经验，并且在很多情况下都曾多次应用且行之有效。关于网络和数据安全的文献浩如烟海，除了解释信息安全的概念外，提供的信息安全解决方案却五花八门，无论是初学者还是经验丰富的网络管理员都感到无所适从。与此相比，本书则给出了一套简单明了的规则，它们对于更好地维护信息安全非常重要。本书基于作者多年来在实现网络解决方案和解决安全问题中的思路和经验，编辑出一套比较完整的规则，以构成保护信息安全的“最佳实例”。

这套最佳实例可以作为建立网络和信息安全机制的“处方”，但并不是解决问题的唯一方法。因为每个网络的配置和安全策略都不同，有些书籍虽然对不同的信息安全解决方案进行了比较，但是很少推荐解决方案，本书把这些最佳实例提炼成一套规则，尽量减小了对环境的依赖，以覆盖可能遇到的大多数环境，但有一些特殊环境除外，例如军方的多级安全。希望本书能够揭开配置信息安全解决方案的神秘面纱，并向初学者和有经验的网络管理员提供一个可以遵循的框架，以便他们对其网络和数据环境进行调整。遵循这些实例需要具有奉献精神并为之付出辛勤的劳动。但是，即使只使用本书中的部分“最佳实例”也会多少提高系统和网络的安全性。

# 目　录

# 第一章

# 信息安全、攻击和网络的脆弱性

为了更好地理解实施信息安全的重要性，本章首先列举了一些黑客可能发起网络攻击的例子。后续章节中提出的信息安全最佳实例可以帮助读者防止这些网络攻击，并减少网络的脆弱性。

注意：如果读者怀疑自己的网络受到攻击，请马上翻到第 19 章“对抗攻击的紧急事件规则”查询可采取的措施，以缩短故障持续时间，防止信息受到破坏。

## 垃圾邮件

垃圾邮件是指可识别或不可识别源向用户站点发送的大量电子邮件。在非恶意形式中，它包括向站点中的很多账号发送大量广告邮件，甚至一天之中多次发送。在恶意形式中（例如电子邮件炸弹），攻击者发送大量邮件，直至目标邮件服务器耗尽磁盘空间。此类攻击消耗目标站点的部分或者全部通信带宽，并且企图通过使邮件服务器繁忙和耗尽磁盘空间来实现邮件服务器的拒绝服务。当磁盘空间耗尽后，邮件服务器将无法再接收其他任何邮件。这种攻击存在一种变形，即黑客向邮件服务器发送一条包含大量转寄地址的邮件消息，一些邮件服务器将会复制该消息，并且试图将其发送到被转寄的目的地址，即使消息发起者的账号不合法。

## 病　毒

计算机病毒是一种简洁紧凑的软件包，为了能够复制并造成破坏，它需要一个宿主（即计算机）。病毒能够攻击计算机软件的任何部分，例如：引导分区、操作系统、文件分区表、EXE 文件、COM 文件和应用程序宏。引导分区病毒用病毒代码替换原有的引导分区，并将其重新定位到其他磁盘空间中，并覆盖该空间上的原有数据。EXE 和 COM 文件病毒则将病毒代码插入或者附加在这些文件中。

有些病毒通过修改原文件结构或者保证不改变 CRC(Cyclic Redundancy Check)来添加病毒代码。尽管某些病毒可能不会给系统操作带来灾难性后果,但是用户最好还是将它们清除,虽然这需要花费一些时间。清除病毒就是要将它们从计算机、软盘和其他与被感染设备进行过数据交换的系统中删除。

## 拒绝服务攻击

拒绝服务攻击不断消耗系统资源,直至系统或应用程序停止工作,从而使计算机系统瘫痪。垃圾邮件或同步分组攻击(即 SYN 洪泛攻击)就是两种最常见的拒绝服务攻击(见 1.10 IP 欺骗)。

## 口令猜测

很多黑客都是通过猜测口令非法进入远程计算机系统的。令人吃惊的是很多系统账号采用的都是弱口令。大多数黑客通过猜测那些使用常见的姓名或者字母组合的口令来获得对系统的访问。黑客通常使用口令生成程序来自动产生口令(通常是一个字典上的词汇),从而获得访问权限。如果访问被拒绝,该程序会生成另外一个口令并重复该尝试过程。这些口令生成程序通常会先尝试一些常用的词汇,例如姓名、行星名和地名等。

## 蠕 虫

黑客一旦进入计算机系统,就能将一种可自我复制的程序植入计算机中,我们称这种程序为蠕虫。蠕虫程序不断进行自我复制,直至塞满所有的磁盘空间和内存。此类程序可以自动搜寻未使用的系统资源,然后将它们耗尽。

## 后 门

黑客一旦进入计算机系统,就可以将一段代码插入系统以创建秘密后门,此后门允许未授权的访问。黑客可以在系统上安置一个程序,它允许随意地通过后门进行访问。当然,黑客也可以为他自己创建一个貌似无害的账号,从而在任意时刻非法访问系统。

## 清除器

黑客使用一种叫做清除器(sweeper)的程序来删除系统中的所有数据。

## 嗅探器

嗅探器是一种监控网络传输数据(即信息包)的程序,它能够收集用于攻击的有用信息。黑客通常使用嗅探器来捕获 telnet,ftp 和 rlogin 的开头数百个字节的

内容，以便获取明文形式的口令和其他有用的信息包信息。黑客一旦攻破某台计算机，并在其上安装好嗅探器，就可以攻击网络中其余所有的机器。

## 分组伪造欺骗

这种形式的攻击会对数据包中的数据做出微小的改动。黑客高手通过更改数据来破坏目标系统。这样通常会导致目标系统接收到被黑客修改过的错误信息（即误报）。从攻击者的角度来看，给目标系统一些错误信息比没有给出信息强。

## IP 欺骗

SYN 洪泛攻击是 IP 欺骗的一种形式，它利用的是 TCP/IP 中每个 IP 连接都会建立的“三次握手”。在这种攻击形式中，黑客将带有一个欺诈源地址的 SYN 分组发送给目的主机，借此来伪造自己的身份。目的主机用这个被伪造的地址将 SYN-ACK 分组发送给可信主机，然后等待 ACK 分组直至超时。目的机器的连接缓冲区会被不完整的连接塞满，直至停止接收新的连接。在这种攻击的另一类变体中，黑客会探测计算机的端口。当发现一个激活的端口时，他就会发送多个 SYN 分组来获得返回 ACK/SYN 分组的序号。然后，黑客假扮成可信计算机，发送另一个 SYN 分组，以及具有正确序号的 ACK，从而建立起到目的主机的连接。一旦目的主机相信该连接是可信的，它就会将信息传递给黑客。

## 特洛伊木马

特洛伊木马是一种可以通过“前门”进入计算机系统的软件代码。这类软件一般嵌入在用户认为无害的程序中，例如文本编辑器或者实用程序。用户会借助这些程序来完成任务和解决问题。这些被嵌入木马的程序在运行时可能会执行特定的恶意功能，例如删除或者拷贝文件到其他计算机中。

# 第二章

# 关于攻击的剖析

本章将给出一个实例，介绍黑客怎样发现信息并且获取对网络的访问权。那些针对系统的攻击可能来自组织内部，也有可能来自组织外部。仅仅保护系统免受外部攻击可能会是安全策略中一个致命的缺陷。不过，大多数攻击确实来自外部一些有经验或没经验甚至新出道的黑客，而且这些攻击多发生在深夜，因为在那时攻击被检测到的风险较低。那些黑客用来入侵网络和系统的工具都可以在因特网上找到。通过对该实例的描述，作者希望读者能够明白，黑客可能会采用一些非常聪明的手段来获取对系统和网络的访问权。更多的详情请参见本书后面列出的参考书目[Meinel98]和[Abene97]。

①黑客选择一个攻击目标。

②黑客试图通过向 InterNIC(因特网网络信息中心)发送 whois 查询来发现该目标组织的因特网连接，进而找到该组织的 DNS(域名服务)服务器。

③向该组织的 DNS 服务器请求 DNS 区传递(zone transfer)。这是一种进入组织内部的探测，不会被组织的防火墙所阻拦(假如他们真有防火墙的话)。

④黑客使用一个能够追踪路由分组路径的程序来探测站点，进而发现过滤路由器的 IP 地址，这个路由器就是目标组织的因特网网关。在探测器发出的分组被拦截之前，组织的内部路由器或者防火墙便成了最后的希望。

⑤试图找到防火墙外部的堡垒主机(见 5.3)的 IP 地址。

⑥扫描堡垒主机的端口，以确定哪些端口是被激活的，以及正在运行的系统服务中哪些能加以利用。

⑦如果获得对主机的访问权，就可以在账号数据库或者口令文件中搜寻存在的用户名。

⑧使用口令破解程序来设法破解管理员或者“超级用户”的账号。访问权限的获取意味着计算机被彻底攻陷，黑客就可以为所欲为了。

⑨接下来，为了入侵网络上的其他机器，黑客会运行一个口令解密程序来获取其他用户名的口令。堡垒主机上一些相同的口令可能会在防火墙内部的机器上使用。通过检查堡垒主机上的“hosts”文件或者其他等效文件，就有可能找到内部机器的地址和名称。

⑩获取这些信息之后，黑客便会通过被攻陷的堡垒主机来试图访问内部机器。被错误配置和弱配置的防火墙是普遍存在的，这些漏洞能被聪明的黑客利用来访问内部网络。如果能够远程登录内网的任何一台主机，就可以在内部机器上运行嗅探器程序，从而发现在网络上传输的明文形式的口令，并因此实现对所有内部机器的入侵。

⑪一旦内部的原始入侵点被发现，内部网络的其他访问点（例如其他防火墙或者带有 Modem 的机器）将会被保护起来。Modem 的电话号码在内部可能是公开的，或者发布在管理员的目录里。另外，将运行一个可以通过扫描电话线来查找 Modem 载波的拨号程序。使用 Modem 的内部 PC 是一个潜在的完美的后门。

⑫攻击过程会尽其所能危及更多的计算机，其最终目的就是占领组织中运行最关键业务的机器并获取敏感信息。

# 第三章

# 安全意识和管理责任

实现信息安全的第一步是创建一个安全策略。然而，在此之前，组织的管理层必须考虑安全风险：安全缺陷将会对组织造成多大的影响，例如公司网站被黑时公众声誉受到的负面影响和潜在的财务风险。还有一些行业，例如医疗卫生，根据法律要求也需要实现信息安全。如果不能高度重视组织面临的安全风险，或者不相信风险的存在，就不可能有效地推行或者维护组织的安全策略。

组织的管理层在很多时候往往没有意识到这些风险，或者不能完全理解它们。由于某些原因，这些人可能不相信组织容易受到攻击。例如，一些小公司的经理往往不会重视安全风险。作者发现在所有级别和类型的组织里，都普遍缺乏对安全风险的管理意识。最好把安全问题看作一件虽然讨厌但又不得不做的事（necessary evil），最坏的情况下它被视为是一次代价极大并且不希望发生的入侵。它必须被看作组织的整体业务策略的一个有机组成部分。管理者必须意识到安全风险通常意味着业务的损失、生产率的降低、数据的丢失、公司机密的泄露，或者公司的整体利益受到危害等问题，必须切实地认识到这些来自黑客的威胁。必须向管理者灌输类似机构近期遭受黑客攻击的实例，从而引起他们对这一问题的足够重视。

如果管理者不同意建立并执行安全策略，那么即使加强安全措施也无法遏制高风险的威胁。这些威胁和减轻威胁所要付出的代价都必须准确、全面地表述出来。只有这样，管理者才能作出一个好的决策。因为需要让管理者认识到威胁以及它对组织的影响，最有力的论据就是清楚地说明可能遭受的财务风险。在必要的情况下，可以聘请一个第三方来分析可能受到的攻击，因为第三方的分析结果通常会对管理层产生更大的影响。

# 第四章

# 安全策略



建立安全策略是保护计算机网络的基本要求，即收集和整理一套最低限度的安全要求，将其作为安全策略的基本原则，这是非常有必要的。该安全策略必须具有可操作性，并且会给运行和网络监控带来一定的额外开销。这些额外开销或收益必须要得到组织管理层的理解和支持，以便于加强、维护网络和系统的安全。

缺乏公认的、深思熟虑的安全策略和指导文件，是当今大多数公司主要的安全弱点之一。本章将讨论有关此类文件的几条最佳实例。此外，附录 B 和附赠光盘中提供了一个通用的安全策略。当然，也不能太过分强调安全策略的重要性。

## ✓信息安全最佳实例# 1

**对目标组织进行威胁分析和风险分析，以确定必须实施的安全级别。**

首先，识别出所有对目标计算机和网络所构成的威胁；其次，确定威胁的种类；再次，进行风险评估；最后，推荐应对措施。我们通过建立一个如图 4-1 所示的“后果/可能性”的矩阵，来进行这个风险评估。

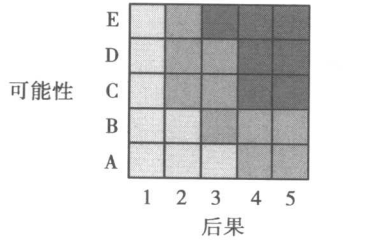


图 4-1　风险等级矩阵

为每种威胁建立一个“可能性/后果”表。产生威胁的“可能性”分为：A = 可能性极小、B = 不太可能、C = 有可能、D = 很有可能、E = 几乎确定。威胁的“后果”等级使用一个计分系统：表中的块 1 = 0 ~ 1 分，块2 = 2 ~ 3 分，块 3 = 4 ~ 6 分，块 4 = 7 ~ 9 分，块 5 = 9 ~ 11 分。这些得分基于对安全损害的主观评估，并按照对组织机能和数据损失的影响来进行划分。例如，5 分 = 组织逐渐停止运

行,关键业务系统丧失功能;3 分 = 部分应用程序停止运行,非关键业务系统丧失机能,但组织仍能运行;0 分 = 未丧失任何功能。数据威胁的判分如下,例如,2 分 = 敏感数据被外人获取;1 分 = 敏感数据被组织内不具访问权限的人获取;0 分 = 没有任何数据损失。有了这个矩阵,需要加强安全性的地方就可以立即凸显出来。当然,还要创建并填写一些其他表格:①标识这些威胁;②提出针对威胁的解决方案;③标明威胁发生的可能性(即 A,B 等);④给出威胁对组织功能和数据的影响;⑤给出损失的后果。

## ✓信息安全最佳实例#2

**为整个站点定义一个安全策略,并且将其作为网络安全体系的指南来使用。**

定义一个如下的安全策略,包括:机密性、完整性、可用性、可核查性、安全保障和实施。该策略应该根据自身的风险和承受能力来涵盖尽可能多的方面。本章所描述的通用安全策略是由 DoD 5200.28 和 SECNA VINST 5239.3 发展而来的。

机密性——系统必须通过控制对信息、服务和设备的访问,来确保敏感信息的机密性。只有具备适当授权并且需要这些信息和服务的员工才能访问该系统和数据。系统必须具备一些特殊功能和程序来对可能危及系统的一切信息、服务和设备实施访问控制策略。

完整性——系统必须保持信息和软件的完整性(即不存在未获授权和未检测到的修改),以确保它们能在网络或者公共访问传输介质上进行适当的处理、存储和传输。系统中的每个文件或数据集,在其生命周期内都必须具备一个可识别源。系统还必须确保执行关键任务的设备的完整性,必须使用自动或手动的安全装置来检测和防止无意或恶意的破坏或修改数据。

可用性——系统必须确保免受拒绝服务攻击的威胁。保护措施必须与其提供的服务和信息的价值相称。必须保护系统免受环境的威胁,例如断电或温度过高等。

可核查性——系统必须支持对所有与安全相关的事件所进行的跟踪,包括违反和企图违反安全策略的子系统、用户以及外部连接等。系统必须执行以下规则:

①连接到本系统的员工和系统必须能被本系统进行唯一识别,在被允许访问敏感信息、服务和设备之前必须具有鉴别标识。

②每个处理敏感或者关键业务信息的子系统,都必须保持与安全相关事件的审计踪迹,包括阻截个人用户或者接口子系统通过未授权接口获得访问的企图。

该审计信息必须能够防止篡改，并保证持续有用。

安全保障——必须鉴别被处理的关键而敏感的信息、设备、服务以及需要知情的员工，以确定适用的安全要求。选用的安全手段必须为关键数据提供足够安全的保护措施，以与安全策略相一致。

实施——在系统的整个生命周期中都必须始终贯彻既定的安全策略。必须对系统安全功能的所有措施，包括在子系统中采取的措施进行评估，以确保能够充分地满足安全策略的要求。每个平台都必须进行评估，以确保系统配置能够正确执行所声明的安全策略。评估结束后可以得到一份系统脆弱性评估报告。该评估结果必须由安全经理或者系统管理员进行评判，以确定是否需要对系统进行修改，以使其能够遵循安全策略。在系统的整个生命周期中都应参考本书提出的信息安全最佳实例，以确保系统能够持续遵循既定的安全策略。为了将安全理念融入设计之中，在新的系统工程的计划和预设计阶段就应充分考虑信息安全因素。



## ✓信息安全最佳实例# 3

**制定一个计划来实施既定的安全策略。**

一旦安全策略被建立起来，就必须制定相应的实施计划。逐步、分阶段地改善基础设施和雇用新员工（如果需要），这将有助于管理开支计划的实施和制定执行时间表。

实施计划应该包含以下步骤：

①确定执行指导方针。这些方针会指明接收安全警告的人员、应采取的行动、事件扩大的命令序列以及报告需求。

②对职员、顾客等进行安全策略方面的培训。

③购买需要的硬件或软件，雇用需要的员工。

④安装和测试设备或软件。