科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

网络安全评估

从漏洞到补丁

Steve Manzuik, André Gold, Chris Gatford 著
张建标 施光源 张国明 译

Network Security Assessment
From Vulnerability to Patch

科学出版社

Network Security Assessment
From Vulnerability to Patch

网络安全评估
从漏洞到补丁

Steve Manzuik　André Gold　Chris Gatford　著
张建标　施光源　张国明　译

科学出版社
北京

图字：01-2008-2614 号

This is a translated version of
Network Security Assessment: from vulnerability to patch
Steve Manzuik, Chris Gatford, André Gold

ISBN-10：1-59749-101-2
ISBN-13：978-1-59749-101-3

图书在版编目(CIP)数据

网络安全评估：从漏洞到补丁/(美)曼佐克（Manzuik，S.）等著；张建标等译. —北京：科学出版社，2009

（21 世纪信息安全大系）
ISBN 978-7-03-023241-0

Ⅰ. 网… Ⅱ. ①曼…②张… Ⅲ. 计算机网络-安全技术-技术评估
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 164121 号

责任编辑：田慎鹏 霍志国/责任校对：林青梅
责任印制：钱玉芬/封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2009 年 1 月第 一 版 开本：787×1092 1/16
2009 年 1 月第一次印刷 印张：14 3/4
印数：1—4 000 字数：349 000

定价：42.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

主要作者

Steve Manzuik 目前在 Juniper 网络公司任高级安全研究主管。他在信息技术和安全行业有超过 14 年的经验，尤其侧重于操作系统和网络设备。在加入 Juniper 网络公司之前，Steve 在 eEye Digital Security 公司任研究经理。2001 年，他成立了 Entrench Technologies 公司，并任技术领导。在 Entrench 之前，Steve 在 Ernst & Young 公司的 Security & Technology Solutions Practice 部门任经理，他是 Canadian Penetration Testing Practice 部门的 solution line leader。在加入 Ernst & Young 之前，他是世界性组织“白帽黑客”的安全分析师，并在 BindView RAZOR Team 任安全研究员。

Steve 是“*Hack Proofing Your Network*”（Syngress 出版社出版，1928994709）第二版的合著者。此外，他在 Defcon，Black Hat，Pacsec 和 CERT 等世界性会议上多次演讲，并且他的文章在许多行业出版物上（包括 CNET，CNN，InfoSecurity Magazine，Linux Security Magazine，Windows IT Pro，以及 Windows Magazine）被引用。

合 著 者

André Gold 目前在 Continental Airlines 公司任信息安全主管，该公司是世界上最大和最成功的商业和货物运输服务商。André 是由该公司以前的 CIO 直接任命的，这使他成为该公司 50 年历史上第一个就任该职位的人。作为信息安全主管，André 建立了一个基于风险的信息安全项目来提高超过 42 000 名员工的安全智商（IQ），以及保护价值 2.5 亿美元的 continetal.com 公司的财产。

作为一个知名的安全从业者，André 在 SC，Information Security，以及 CSO Magazine 起了重要作用。André 也出席或参加了许多行业相关的会议。2006 年，由于 André 在信息安全领域的初期工作和对运输市场的贡献，他在零售业被授予 Information Security 7 奖。

在从事现在的工作之前，André 在 Internet and Network Services 公司任技术主管。任职期间，他负责并建立了 Continental 公司的基础设施和 continental.com 公司的财产，该财产占了公司总收入的接近 25%。

业余时间，André 在科罗拉多州攻读了 MBA，并且在 Houston-Downtown 大学攻读了计算机信息系统的 BBA。André 也曾从 Wentworth Military Academy（Wentworth 军事学院）收到委任状，在部队做过军官。

除了在 Continental 的工作，André 还为以下组织服务：Microsoft Chief Security Officer Council，Skyteam Data Privacy and Security Subcommittee，Goldman Sachs 安全顾问，以及 eEye Digital Security 和 ConSentry Networks 的执行顾问。

编　者

Chris Gatford　他在位于澳大利亚悉尼的 Pure Hacking Ltd 公司工作，是世界上许多组织进行渗透测试的高级安全顾问。Chris 检测过无数 IT 环境，并且直接领导和负责了许多企业及政府部门的安全评估。

Chris 是课程“Pure Hacking OPST”的讲师，此前在 Ernst & Young 工作，并且作为“eXtreme Hacking”课程的首席讲师。在这两个职位上，Chris 向来自全世界各个组织的上千名学生讲授了专业黑客的艺术。

Chris 经常在与安全相关的学术会议上演讲（最近出席的会议是 AusCERT 2006）。他是许多安全专业组织的成员，并且取得了 CISSP(Certified Information Systems Security Professional）认证。更多详细的相关信息可以从他的主页 www. penetrationtester. com，以及目前所在公司的网站 http://www. purehacking. com 获得。

Ken Pfeil's　他从事 IT 和安全工作 20 多年了，在很多公司工作过，如 Dell，Avaya，Identix，BarnesandNoble. com，Merrill Lynch，Capital IQ，Miradiant Global Network。在 Microsoft 工作时，他与别人合著了 Microsoft 的“Best Practices for Enterprise Security”白皮书系列。Ken 为许多书籍做出了贡献，包括“Hack Proofing Your Network”第二版（Syngress，1928994709），“Stealing the Network：How to Own the Box”（Syngress，1931836876）。

Bryan Cunningham　（JD，Certified in NSA IAM，Top Secret security clearance）他在信息安全、情报及国家安全领域拥有丰富的经验，是任职于美国政府和私营机构的高级职员。Cunningham 是企业信息和国土安全顾问，并且是丹佛的法律公司 Morgan & Cunningham LLC 的负责人，最近他是国家安全顾问康多利萨·莱斯的代理法律顾问。在白宫，Cunningham 起草了《国土安全法案》的关键部分，并且参与制定了“National Strategy to Secure Cyberspace”（《保护网络空间的国家战略》），以及许多总统领导的关于空间安全的法案。他是前任中央情报局官员、联邦检察官，还是 ABA CyberSecurity Privacy Task Force 的共同创办者。2005 年 1 月，由于他在信息领域的成就，他被授予国家情报局成就勋章。他已经被委派到国家科学院学术委员会，在 Biodefense Analysis and Countermeasures 部门工作，并且是美国安可顾问公司（APCO Worldwide Consulting）的资深顾问，也是 Markle Foundation Task Force on National Security in the Information Age 的成员。他为公司的信息安全项目及其他国家安全相关问题提供咨询，作为信息安全顾问来指导并监督信息安全评估工作。

译 者 序

随着计算机和网络技术的迅速发展，尤其是互联网的快速发展，人们对网络的依赖达到了前所未有的程度，网络安全越来越显示出重要性。近几年来，网络安全面临越来越严峻的考验，如何保障网络安全显得非常重要，而网络安全评估是保证网络安全的一个重要环节。

本书的各位作者都有多年的信息安全从业经验，并担任各个大型公司主要的信息安全职位，书中融合了他们的实践经验，与单纯的理论教科书不同，提供了从理论到实践的有机衔接。本书从漏洞评估、漏洞评估工具、漏洞评估步骤和漏洞管理等方面介绍了网络安全评估所涉及的方方面面。通过本书的学习，一方面可以使读者了解网络安全评估的一些基本概念、基本原理，另一方面更重要的是可以实际指导读者一步步地完成整个评估过程。此外，书中介绍了网络安全评估中各种常用的开源工具和商业工具，以及对各种工具的特点比较分析也有助于读者能够快速地找到合适的评估工具，这点对初学者尤其重要。从写作风格上，本书的最后一章又从总体上概括了网络安全评估的整个过程，可以在实施网络安全评估时作为必要的参考手册。

本书适合作为信息安全高年级本科生或研究生的教材，也可以作为相关领域专业人员的参考书。

本书由张建标教授组织翻译，参加翻译的人员还有施光源、张国明，最后由张建标负责统稿和审校。

由于译者的水平有限，书中翻译不妥或错误之处在所难免，恳请广大读者批评指正。

译者

2008 年 12 月

序　言

我已经以多种方式公开从事有关计算机和软件漏洞方面的工作十多年了。在非公开场合，我似乎一生都在参与计算机及其他相关方面的工作。我通过 L0pht 组织发表了一些早期的建议。有些报告被送往了政府部门，有些攻击和防御工具发布出来，从 L0PhtCrack 到 Anti-Sniff，再到 SLINT，还有一些个人和工作专用工具。保护备受关注的各种网络，无论是大型的还是小型的网络，都是平常事，受命侵入防御坚固的网络更是平常。但是只关注这些事情的本身并不能得到什么信息。通过不断对更全面情况的理解（也就是说，所有变化的部分如何从技术层面一直到项目经理和公司态度都能够相互联系）可以制定出实际的目标。不管攻击者还是防御者，都会遇到这个问题。

发现漏洞是很有趣的事情，多半是因为所要寻找的是鲜为人知的东西。过去，人们并不总是想把如何发现安全漏洞的信息隐藏起来，而是因为漏洞搜查还是一个新兴领域。现在，有大量的网络和出版文档可以用来处理一般的和特殊的安全漏洞。但是从更加广阔的角度来看，这种资料真正地能告诉读者什么，并且如何与读者在现实世界的情况联系起来？这种资料如何能让负责一个公司小组或者是整个公司的人来做好他们的工作？

让一个攻击者搜寻漏洞有什么风险呢？很多情况下，攻击者可以获得要进攻的软件或者操作系统的一份拷贝，然后在自己的测试环境中进行测试，这样搜寻漏洞的风险很小。这种情形也经常发生。然而，现实的世界毕竟与实验室环境不同。对于攻击者而言，复制一个特定的环境可能是不可行的，因为这太过于复杂且需要精心策划。可能目标环境是完全未知的。在这些情况下，人们乐于探索和实验不属于他们的实用系统时有何种风险呢？除了搜寻实用外部系统中未知漏洞存在的风险，试图利用这些漏洞还有什么风险吗？是一个系统崩溃还是引起攻击者注意？网络是否变得过于拥挤，不仅阻止合法用户使用，而且也阻止攻击者使用网上的服务和资源？

在一个真实的环境中，有多少种破解的机会留给攻击者？组织提供的服务和系统是否在任何时候，任何地方都是可用的？在进行维护和回滚的时期，有可变的机会窗口吗？这个机会窗口会受到软件升级和版本更新的限制吗？成本同样会影响机会成分。有些举措可能在财政上是不允许的，如果其他一些举措以开发、交付和使用的时间段作为成本标尺，则可能太昂贵了。

何种动机驱使攻击者对你的环境感兴趣呢？对有些人而言，可能是机会主义的想法；然而对其他人而言，他们都有明确的目标。可能有人受命于一个国家、竞争对手或者基于某种特定的信念。或者有些人就是无聊，这对你来说就不走运了。

这种特殊的对手模型技术也称之为 ROM（风险、机会及动机）模型，是非常强大的。它开始考虑对手目标更多的组成部分，并对应到现有真实世界的环境中决定用来防范或取证的重要地点和各种措施。这个模型有一个好处是在没有考虑环境、对手目标，以及没有对模型存在的问题和环境进行鉴定的情况下，就不必考虑一个漏洞，并且也不用考虑可能受命攻击或者防御的网络和系统里存在的问题进行处理。

可能你已经知道如何去寻找漏洞，可能不仅善于在人造的实验室环境里测试，而且

也能在复杂的交互系统上进行测试。实际上，为正在对付的敌人构建模型并理解它与现实中存在的许多模型一样，是让人感到舒服的任务。如何处理风险，应该知道风险已经披露给某些已经定义的敌人及一些该忘记的敌人。我见过针对不同情形的很多不同解决方案，那时有些方案让我很是吃惊。

例如，一个拥有1000名员工的公司刚刚被一家更大的公司收购，收购之后不久，这个较小的公司被告知要给收购公司的一个大的业务部门提供自由的访问权限。经过快速地检查之后，安全指导人员注意到，这个业务部门用来阻止主要来自因特网的非授权访问的网络保护实际是不存在的。对这种情况给出的建议是不允许该业务部门自由地访问，直到能够改善它在网络接入点的安全状况为止。但结果是要求刚被收购的公司把安全防护水平降到最低的通用标准，这种做法意味着业务部门的防御将是千疮百孔。由于缺少更全面的资料（非常像只是理解一个漏洞本身，而不考虑把它放在一个存在潜在攻击者的环境中，进行各种操作需要兼顾公司的生存，有各种目的的对手，以及进行修补工作的成本等因素），这种做法是非常幼稚的。在我任安全领导的时候，曾经给一个较小的公司内化过ROM模型，而且不认为大公司可能会与之不同。后来证明，放弃所有用于阻止业务部门获得自由访问权限的安全过滤器和各种举措是正确的解决方案，为什么？存在问题的业务部门是刚刚完成收购的公司的最主要的赚钱机器。这个业务部门已经带来了数十亿美元的收入，当然还将再带来更多的收入，这个部门需要承担某些风险。虽然让网络处于相对开放和易受攻击的风险状态可以说不能被业务部门完全理解，但它已经把很多安全因素计划到了很细微的层次。这个大公司所做出的决定是愿意接受网络欺诈及每年数百万美元的损失。被收购的小公司，包括所有的收入和资产，被建模到这个模型中且已经做出说明。降低网络安全标准可能会让业务部门大幅提高利润，而由于网络攻击或者危害造成小公司的损失是可以接受的。在受到这些启示不久之后，安全小组会提供所有权限，这并不是说取代所有的安全防御措施，因为没有足够的资金来实施监控和部署从而确保漏洞被快速地发现。因而，当各种不可避免的问题产生时，快速地提出解决方案，包含和实体化所有风险是很有意义的。

当本书作者与我联系并解释他们将尝试写什么的时候，我非常高兴。我不知道是否有一本书可以涵盖所有的涉及安全防护方面的令人深思的方法，这些方法是人们在真实的世界中所涉及的信息安全的方方面面。解释的概念不仅包括什么是代码中的一个漏洞，还要解释如何发现它（何种工具可以帮助发现）和测试它（理解和分类所保护的网络环境），如何去管理和处理知道的和不知道的漏洞（但是会以一种不太令人愉快的方式发现），或者修补和重构系统……如果有大量可用的书籍涵盖了上述问题，而且这些书是权威人士早在我写本书以前的，我会很高兴地去拜读。

Cheers,

. mudge (Peiter Zatko)

Technical Director, National Intelligence

Research and Applications division of BBN,

former advisory to the White House and Congress,

author of LOphtCrack,

and founder of @stake and Intrusic

目　录

第 1 章
漏洞窗口

本章主要内容：

- 什么是漏洞？
- 理解漏洞造成的风险

- √ 小结
- √ 快速解决方案
- √ 常见问题

引言

本书不是典型的介绍信息技术（Information Technology，IT）安全的书。虽然本书作者具有专业技术背景，而且也写过一些很畅销的书，如 Syngress 出版的“*Hack Proofing Your Network*”，但是本书还是主要将漏洞管理的技术融入到业务管理中。尽管熟悉最新的黑客技术是很重要的，但是只有当能够把黑客所实施的威胁与对组织所造成的风险联系在一起时，这些知识才是有价值的，本书将介绍做这件事情的工具。

本章主要介绍漏洞及其重要性，我们还将讨论一个被称作“漏洞窗口”（Windows of Vulnerabilities）的概念，以及如何确定一个已知的漏洞对环境造成的风险。

什么是漏洞？

那么，什么是漏洞呢？在过去，很多人把漏洞看作是有恶意的人能够利用的软件或硬件的缺陷。然而，在近几年中，漏洞的定义发展成为有恶意的人能够利用的软硬件的缺陷及配置错误（misconfiguration）。补丁管理、配置管理和安全管理等常常相互竞争的学科，都已从单一的学科发展成为同一个信息技术（IT）方面的问题，那就是今天的漏洞管理。

注 释

本书将通过 CVE 编号来引用漏洞。CVE 是 Common Vulnerabilities and Exposures 的缩写，即通用漏洞披露。为了使漏洞命名标准化，人们在几年前制定了一系列的 CVE 编号。在使用 CVE 编号之前，漏洞的名字由厂商随意指定，这使得跟踪漏洞变得困难而混乱。CVE 制定了所有漏洞的一个列表，并且按照 CVE-year-number 的格式给每个漏洞分配一个 CVE 号码。当引用漏洞的时候，鼓励厂商使用 CVE 编号，实践证明这种方式消除了大部分的混乱情况。更多关于 CVE 编号的信息可以查看网站 http://cve.mitre.org。

从表面上看，漏洞管理像是个简单的工作。不幸的是，在大部分组织的网络中，漏洞管理既困难又复杂。一个典型的组织中包含定制的应用、移动用户及关键服务器，它们有不同的需求，不能只做简单地保护，更不能置之不理。软件厂商仍会发布不安全的代码，硬件厂商也不会将安全内建在产品中，因此这些问题就留给了系统管理员来处理。加入这些必须遵守的规定使管理者感到紧张，并且处于一种高压状况下，容易导致犯严重的错误。

针对漏洞管理的复杂情况，人们提出了“漏洞窗口”的概念。尽管这好象是一个聪明的文字游戏，把人们的注意力引向了最常用的 Windows 操作系统，但它实际上指的是一个系统由于安全缺陷、配置问题或导致降低整个系统安全性的其他因素，而处于易