Network Security Assessment

第二版

网络安全评估

O'REILLY®
中国电力出版社

Chris McNab 著
王景新 译

第二版

网络安全评估

Chris McNab 著
王景新 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc.授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

网络安全评估/（美）麦克纳布（McNab, C.）著；王景新译 －2版.
－北京：中国电力出版社，2009.9
书名原文：Network Security Assessment, Second Edition
ISBN 978-7-5083-9079-6

I. 网… II. ①麦…②王… 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（2009）第111529号

北京市版权局著作权合同登记
图字：01-2009-3960号

书　　名/　网络安全评估（第二版）
书　　号/　ISBN 978-7-5083-9079-6
责任编辑/　孙芳
封面设计/　Karen Montgomery，张健
出版发行/　中国电力出版社（www.cepp.com.cn）
地　　址/　北京三里河路6号（邮政编码100044）
经　　销/　全国新华书店
印　　刷/　北京市同江印刷厂
开　　本/　787毫米×1092毫米　16开本　30.5印张　547千字
版　　次/　2010年5月第一版　2010年5月第一次印刷
印　　数/　0001－3000册
定　　价/　58.00元（册）

O'Reilly Media, Inc.介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc.授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc.是世界上在 Unix、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的*The Whole Internet User' Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc.一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc.是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc.具有深厚的计算机专业背景，这使得O'Reilly Media, Inc.形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc.所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc.还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc.依靠他们及时地推出图书。因为O'Reilly Media, Inc.紧密地与计算机业界联系着，所以O'Reilly Media, Inc.知道市场上真正需要什么图书。

目录

序言

在对逾20,000起针对信息基础设施和应用程序的渗透测试进行过绩效管理之后，我越来越认识到技术测试和提供信息安全保障的重要性。

本书精确地定义了一种纯粹的技术评估方法学，阅读本书会让读者对现今的公共网络所面临的威胁、所存在的漏洞及漏洞披露方式有一个更为深刻的理解。我在信息系统安全领域20余年的工作经历中，所进行的数以万计的渗透测试的目的是“识别被测系统的技术漏洞，以便纠正这些漏洞或者降低由这些漏洞所带来的风险”。在我看来，对于为什么要进行渗透测试而言，这是一个清晰简明但也是错误的理由。

阅读本书时，你会逐渐认识到，在大多数情况下，漏洞及其披露源于系统管理不善、没有及时打补丁、弱口令策略、不完善的存取控制机制等。因此，进行渗透测试的主要原因和目的应该是识别和纠正系统管理过程的失效，正是这种失效导致了系统漏洞的出现，并在渗透测试的过程中被披露出来。最常见的系统管理过程失效包括：

- 系统软件配置的失效；
- 应用程序软件配置的失效；
- 软件维护的失效；
- 用户管理和系统管理的失效。

遗憾的是，很多IT安全顾问仅仅提供特定测试所发现问题的详细列表，但从来不尝试进行更高层次的分析，以便回答“为什么会存在这些问题”。缺乏对那些系统管理失效（系统管理失效是引发测试中所发现的问题的本质原因）的识别和纠正所带来的后果是，在六个月之后，当IT安全顾问再一次对信息系统进行测试之后，新的问题又会出现。

如果你是一位负责信息系统安全的专业人员，本书将帮助你评估你所负责管理的网络，本书有效地列出了你的敌人所可能采用的攻击技术和工具；如果你是一位为客户进行安

全评估的顾问，铭记本书中所讨论的那些可能引发系统漏洞的管理过程失效是至关重要的。

多年以前，我的公司曾经为一个大型的国际客户进行过一系列的渗透测试，该客户的业务系统是多区域性的，所执行的IT安全策略是集中发布、分区域执行的。我们把测试得到的技术结果映射到了如下的一些管理范畴：

操作系统配置

由于不正确配置操作系统软件所引发的漏洞。

软件维护

由于未对已知漏洞打补丁而引发的漏洞。

口令/存取控制

由于不遵守口令策略和不正确的存取控制设置而引发的漏洞。

恶意软件

存在恶意软件（木马、蠕虫等）或至少有其存在的迹象。

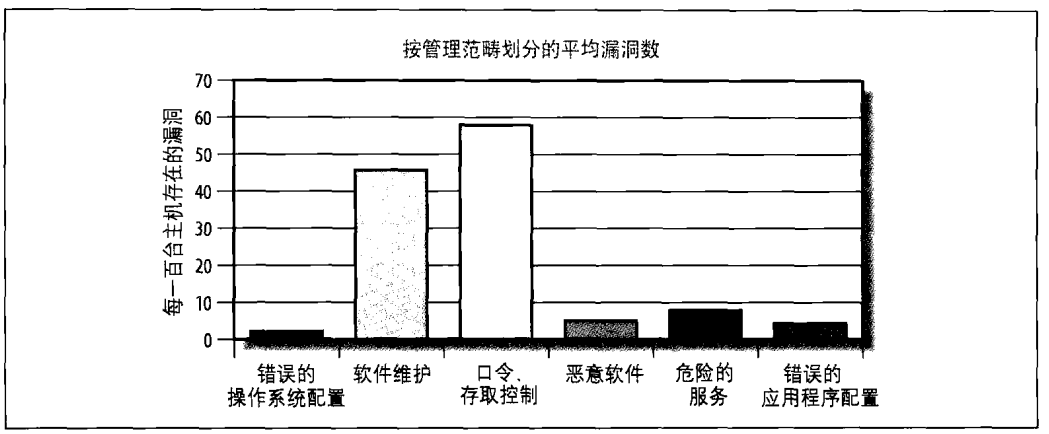
危险的服务

存在有漏洞的或易被攻击者渗透的服务或进程。

应用程序配置

由于应用程序配置不当引发的漏洞。

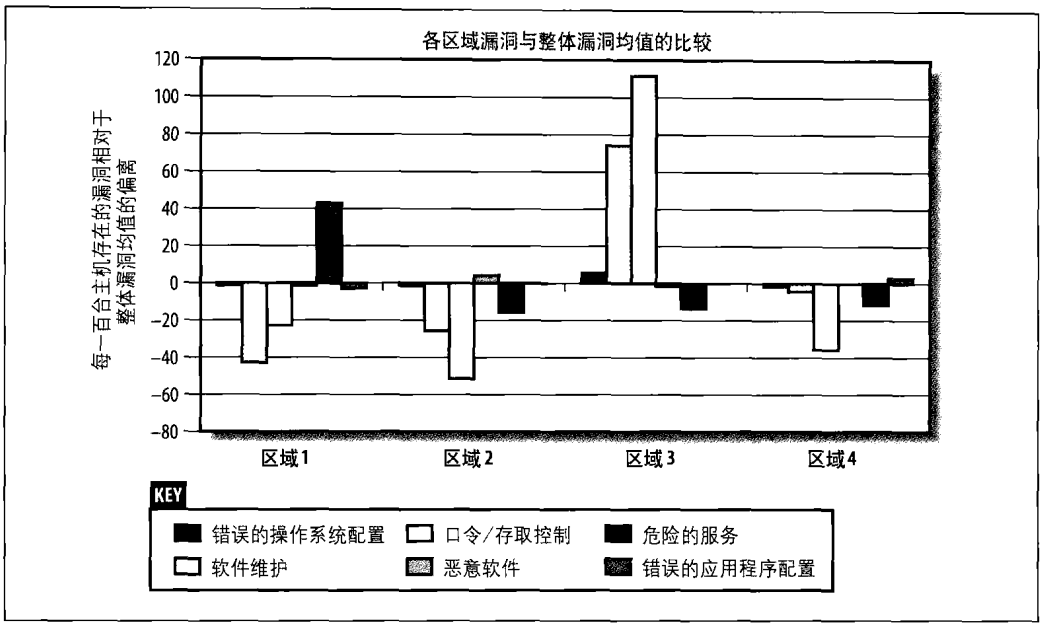
根据评估所得到的结果，我们计算出了由安全评估过程所得到的安全漏洞数的平均值（以整个组织的每一百台被测系统为基数单位），如图F-1所示。



图F-1：根据管理范畴划分的平均漏洞数

在进行上述平均漏洞数的计算之后，为对整个组织内不同区域的信息安全状况进行分析

和比较，我们又对每个区域内存在的系统漏洞数和整个组织存在漏洞的均值进行了比较。结果是很明显的，如图F-2所示（在均值以上被认为是“坏的”，说明该区域存在的漏洞高于整个组织的漏洞均值）。



图F-2：各区域漏洞与整个组织漏洞均值的比较

图F-2给出了由于各个区域所采取的安全管理措施不同而产生的可辨别的、可量化的漏洞差别。例如，区域3的IT管理者显然没有执行有效的软件维护和口令/存取控制管理措施，而区域1的IT管理者则没有从其所管理的系统中去除不必要的服务。

在阅读本书的时候，要重点注意的是，你应该把漏洞及其披露划归到不同的范畴，并且以一种新的视角来对其进行研究。你可以给你的客户提供一份全面地总结了较低层面技术问题的技术报告，但在根本性高层管理失效问题解决之前，网络的安全性并不会得到真正的提高，同时相同的漏洞及其变种以后仍然会出现。本书将向你展示怎样执行基于Internet的安全评估，但至关重要的一点是：你要经常去想“这些漏洞为什么会出现？”

关于Bob Ayers

Bob Ayers目前是英国一家重要的IT公司关键基础设施防护部门的主管。此前，Bob在美国国防部工作过29年，他的主要IT安全职位是在国防情报局（Defense Intelligence Agency，DIA）担任DoD情报信息系统（DoD Intelligence Information System，DoDIIS）的负责人。在任职期间，Bob开发并实现了新的方法学，用于保障40,000多

台用于处理高密级情报资料的计算机系统的安全。Bob还创立了DoD的计算机应急响应机构，即自动化系统安全事件支持组（Automated Systems Security Incident Support Team，ASSIST）。鉴于他在DoDIIS的出色表现，美国国防部助理秘书处（指挥、控制、联络与情报）选择了由Bob来创建并管理一个有155名参与人员、每年1亿美金支持的DoD-wide项目，以从各方面提升DoD的IT安全性。在卸任公职之前，Bob担任美国DoD防御性信息战项目的主管。

前言

对一个黑客而言，闯入计算机系统从来就不是绝对不可能的，而只是有时候不太可能的。

现今，计算机黑客能够经常性地侵入公司网络、军事网络、在线银行以及其他网络化环境。就在2007年，我写作本书第二版时，计算机入侵事件仍处于高发期，我有时仍然要从事应急性的事件响应工作。随着信息系统安全性的普遍增强，黑客所使用的入侵技术也更加高级，包括错综复杂的重新定位、社会工程、物理侵入（从服务器上盗取磁盘或安装无线接入点），还可以使用特定的0day渗透脚本攻击信息系统的外围软件组件，如防毒软件或备份系统，这些组件广泛部署在企业网络内部。

出于同样原因，你可能期待专业的安全顾问来测试这些类型的漏洞与安全问题，但大多数情况下并非如此。之所以这样说，是因为在Matta站点我们运行了一个名为Sentinel的程序，该程序主要对提供金融服务的公司进行安全评估。Sentinel平台包含了大量存在漏洞的系统，对这些金融服务安全评估销售商本身的评估依赖于他们在其中发现与报告的漏洞。

自2004年以来，Matta已经使用Sentinel对全球近30个渗透测试销售商进行了评估。在近期的一次评估中（涉及到10个渗透测试销售商），我们发现了如下一些问题：

- 两个销售商没有扫描所有的65536个TCP端口。
- 五个销售商没有报告公共可访问的MySQL服务的一个root口令“password”。
- 七个销售商没有报告可以轻易渗透的、高风险的SSL PCT溢出漏洞（MS04-011）。

很多销售商都不止一次地经过Sentinel平台的测试，显而易见的是这些销售商缺乏对严格的测试方法学的遵循，从而导致不同销售商的测试结果（特别是提交给客户的最终报告）存在很大差别，这主要依赖于进行测试的安全顾问个人资质。

有鉴于安全评估中存在的这些问题，我决定在2007年对本书第一版进行更新与修订。本

次修订有清晰的目标与定位：归档总结一种清晰、精确的基于Internet的网络安全评估方法学。在多次独立使用Sentinel程序进行了大量有挑战性的安全评估又在Matta建立了一个称职的安全评估团队之后，我感觉现在到了更新本书的合适时间。

概览

本书主要致力于详细地研究和解决整个大的信息安全领域中一个单独的范畴：用结构化的、逻辑化的方法进行IP网络的安全评估。本书所描述的安全评估方法学将描述一个坚定的攻击者怎样急速穿行于Internet上的网络空间，搜索那些存在漏洞的组件（从网络层到应用层），同时也将告诉你怎样对你的网络进行行之有效的评估演练。本书不包含与基于IP网络的安全测试无关的其他信息，战争拨号（扫描）与802.11无线网络评估等内容也超出了本书的范围。

评估是任何一个试图正确管理安全风险的组织所应该进行的第一个步骤。我个人的背景是从十几岁开始黑客生涯，之后逐渐成长为一个专业的安全分析家。实事求是地说，在过去的九年中，我对多家财务服务公司和跨国公司进行网络攻击的成功率是百分之百。在安全业界，我有很多有趣的工作和经验，现在，我感觉应该把这些经验和别人分享并希望能对别人有一些实际的帮助，因此我将在本书中讲述怎样借助其中所定义的安全评估方法学进行有效的安全评估。

通过采用与一个坚定的攻击者相同的方法对网络进行评估，你将能够采用一种未雨绸缪的方法进行安全风险管理。本书包含了密集的检查清单，这些清单包含了相当多的针对攻击者的应对措施，这些应对措施将指导你设计一个清晰的技术策略，并借助该策略在网络层和应用层对你的网络环境进行安全加固。

公认的安全标准

本书的写作遵循在美国与英国使用的政府渗透测试标准，分别为NSA IAM与CESG CHECK。其他一些相关的测试标准包括MasterCard SDP、CREST、CEH以及OSSTMM，这些流行的信息安全鉴定程序将在这里进行讨论。

NSA IAM

美国国家安全局（*National Security Agency*，NSA）提出了信息安全评估方法学（*INFOSEC Assessment Methodology*，IAM）技术框架，以便于NSA之外的安全顾问和安全专业人员能够在遵循公认的评估标准的前提下为客户提供安全评估服务。NSA IAM的主页是*http://www.iatrp.com*。

IAM框架定义了对基于IP的计算机网络进行测试的三个层次：

评估（Assessment）

层次一包含了对被评测组织的整体情况的一个较高层次的概览，主要包括对组织整体策略、组织运作程序和信息流的理解等内容。本层次不对组织的网络或系统进行任何实际的技术性测试。

评价（Evaluation）

层次二是一个实际的、协作进行的过程，其中涉及到通过网络扫描、渗透工具以及某些特定的专门技术的应用进行测试。

红队（Red Team）

层次三的评估是非协作的，同时对目标网络而言是从外部进行的，包括模仿适当的敌手进行的渗透测试等内容。IAM评估是非入侵性的，所以在IAM框架内，本层次的评估包括了对目标网络存在的漏洞的全面量定。

本书只描述IAM框架的第二层（评价）和第三层（红队）所用的网络扫描和相关的评估技术，而对第一层不做描述。第一层往往包括较高层面的协作信息收集，如安全策略等。

CESG CHECK

英国的政府通信指挥部（Government Communications Headquarters，GCHQ）有一支称作通信与电子安全组（*Communications and Electronics Security Group*，CESG）的信息保障力量。与美国NSA IAM框架允许NSA之外的安全顾问为客户提供评估服务的方式类似，CESG有一个称作CHECK的标准，CESG会依据CHECK对英国内部的安全测试小组进行资质评估和授权，使其可以在允许的范围内承担政府的评估工作。CESG CHECK的主页是*http://www.cesg.gov.uk/site/check/index.cfm*。

与NSA IAM不同的是，CESG CHECK涵盖了信息安全领域的很多方面（包括安全策略评审、反病毒软件、备份以及灾难恢复等内容），较之NSA IAM，可以认为CHECK能更全面地应对网络安全评估这一领域。CESG的另外一份标准是CESG列出的指导方案（CESG *Listed Adviser Scheme*，CLAS），这一标准用更为宽广的视野来面对信息安全问题，并能够应对其他的一些领域，如ISO/IEC 27002、安全策略制定、审计等。

为保证对CHECK顾问的正确授权，CESG开展一门攻击实践课程，并通过这一课程来测试参与者所具备的攻击、渗透的技术和方法。公开的CESG CHECK攻击课程笔记列出了与网络安全评估相关的如下一些技术能力：

- 使用DNS信息获取工具处理单个或多个记录，包括对目标主机相关的DNS记录结构的正确理解
- 使用ICMP、TCP及UDP网络映射和探测工具
- 展示进行TCP服务标志获取的技术
- 使用SNMP进行信息取回，包括对与目标系统配置和网络路由相关的MIB结构的正确理解
- 理解路由器和交换机中存在的与Telnet、HTTP、SNMP以及 TFTP 存取和配置机制相关的一些常见的缺陷

下面列出的是针对Unix环境，攻击实践课程的参与者所应该具备的技术能力：

- 示范如何进行常见的用户枚举攻击，包括*finger*、*rusers*、*rwho*以及SMTP等技术
- 使用相应工具枚举远程过程调用（*Remote Procedure Call*，RPC）服务，并对这些服务潜在的安全问题有较为深刻的理解
- 展示对网络文件系统（*Network File System*，NFS）漏洞的测试
- 测试远程服务（*rsh*、*rexec*、*rlogin*）中的漏洞
- 检测不安全的X Windows服务器
- 测试web、FTP、Samba服务中的漏洞

下面给出的是针对Windows NT环境，攻击实践课程的参与者所应该具备的一些技术能力：

- 对NetBIOS、CIFS服务进行评估，以便枚举用户名、组、共享资源、域、域控制器、口令策略以及相关的漏洞。
- 通过NetBIOS、CIFS服务进行用户名与口令破解。
- 检测并展示*Internet Information Server*（IIS）web服务器、FTP服务组件、Microsoft SQL Server中存在的已知漏洞。

本书清晰地归纳总结了对上面所列出的这些领域如何进行评估，同时还阐述了有助于读者正确理解书中呈现的那些漏洞的背景信息。虽然CESG CHECK纲要的出发点是通过这些手段评估那些试图为英国政府进行信息安全测试的安全顾问所具备的方法论和技术手段的有效性，但毫无疑问的是，英国境外的那些组织和公司内部负责安全的技术小组也应该了解这个技术框架以及其中的那些公共知识结构。