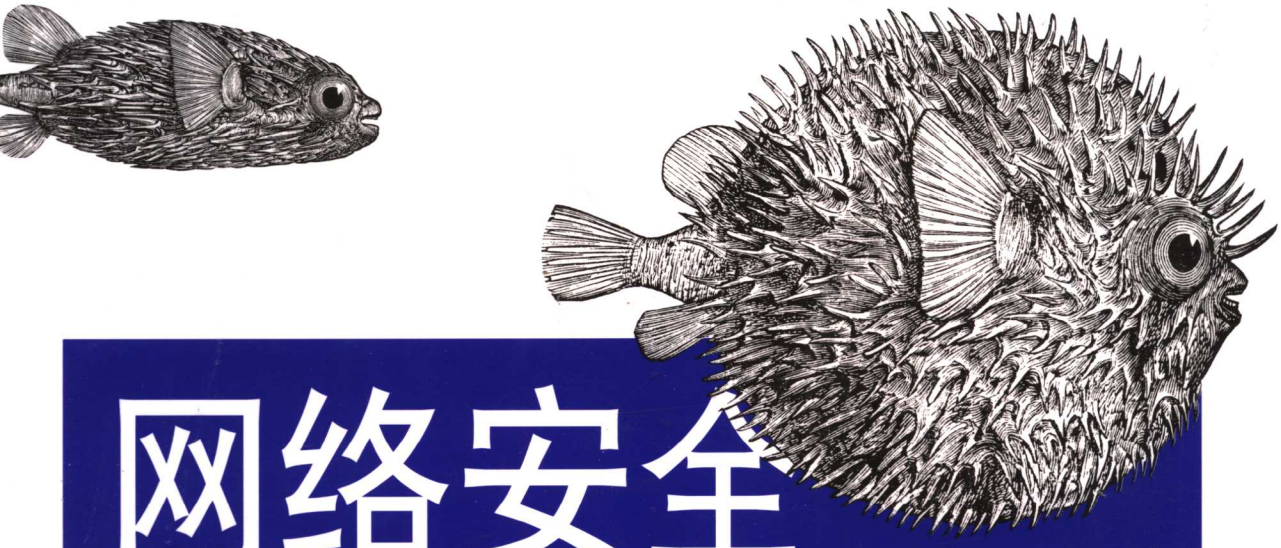
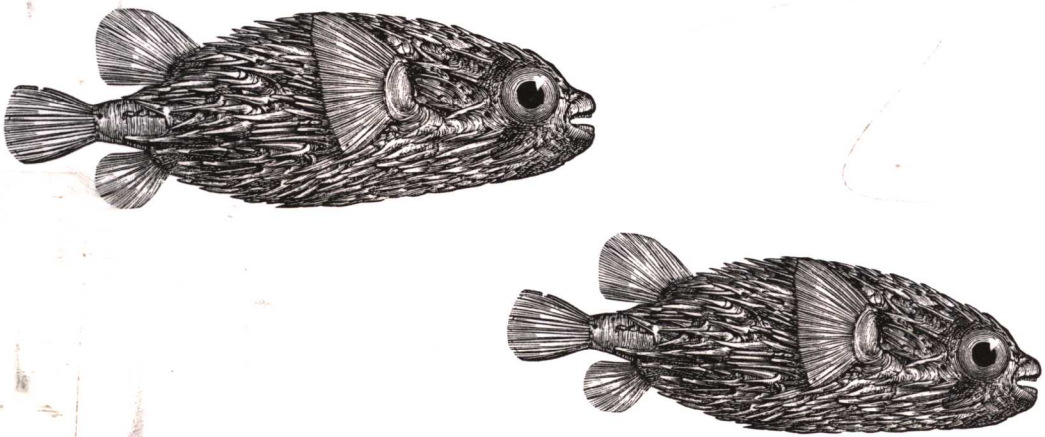
Network Security Assessment



网络安全评估



O'REILLY®
中国电力出版社

Chris McNab 著
王景新 译

网络安全评估

Chris McNab 著
王景新 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • 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）麦肯兰勃（McNab, C.）著；王景新译 －北京：中国电力出版社，2005

（O'Reilly Security 系列）

书名原文：Network Security Assessment

ISBN 7-5083-3861-8

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（2005）第 115687 号

北京市版权局著作权合同登记

图字：01-2005-3232 号

书　　名 / 网络安全评估

书　　号 / ISBN 7-5083-3861-8

责任编辑 / 牛贵华

封面设计 / Emma Colby，张健

出版发行 / 中国电力出版社（www.infopower.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 / 北京市地矿印刷厂

开　　本 / 787 毫米 × 1092 毫米　16 开本　24.5 印张　445 千字

版　　次 / 2006 年 1 月第一版　2006 年 1 月第一次印刷

印　　数 / 0001-4000 册

定　　价 / 45.00 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，同时是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的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。

作者简介

Matta（*http://www.trustmatta.com*）是英国一家独立于各销售商的安全咨询机构，**Chris McNab** 则是该机构的技术主管。自 2000 年以来，Chris 在欧洲境内介绍并开设了应用型黑客教程，以实用的攻击与渗透技术培训了一大批来自金融业、零售业与政府部门的客户，以便使这些客户可以对自己的网络进行有效的评估与防护。

Chris 在很多安全会议和研讨会上进行演讲，并经常性地应邀对安全事件与其他系统闯入等新闻进行评论。在英国的电台与电视台（包括 BBC 1 与 Radio 4）以及很多出版物与计算类杂志上都会看到 Chris 的身影，听到他的声音，见到他的名字。

作为 Matta 机构安全评估服务的提供者和维护者，Chris 及其领导的团队承担着基于 Internet 的、内部的、应用程序的以及无线网络的安全评估工作，并为客户提供关于安全网络设计以及加固策略的实用与合理的技术建议。Chris 不无骄傲地声称，在过去的五年中他对跨国公司和财政服务公司网络的破解率高达 100%。

你可以通过电子邮件 *chris.mcnab@trustmatta.com* 与 Chris 联系。

封面介绍

本书封面上的小动物为刺鲀（二齿鲀科）。这种鱼遍布于世界各地的海洋中，大多数生活在珊瑚礁中或附近。刺鲀的身体一般长度为 3 ~ 19 英寸，上面长着相对较小的棘刺。在受到威胁的时候，刺鲀会不停吸水把胃充满使身体膨胀起来，在数秒之内，刺鲀狭长的身体会膨胀 2 ~ 3 倍，身上的刺也迅速挺立起来（少数种类刺鲀的刺一直是挺立的）。刺鲀的身体上有分布均匀的黑色斑点，这将它和其他河豚区分开来。

刺鲀的上下颚各一颗牙齿，在中间结合，形成一个像鹦鹉的喙一样的吻。刺鲀是夜间的狩猎者，要捕食的时候，刺鲀会将身体移动到沙地上，并喷射出小水柱以吸引猎物。刺鲀同时还是受欢迎的水族观赏动物，有时人们也将其制成标本作为纪念品出售。

在几个世纪前，某些太平洋岛屿上的武士愿意使用刺鲀来装饰自己的头盔。他们首先捕获到刺鲀，由于受到威胁刺鲀会膨胀起来，膨胀之后武士就将其在沙地里埋一个星期左右。再挖出来的时候，刺鲀就变成了一个硬球，武士们将其剖开，并将其制成坚硬的、头状的、看起来非常可怕的饰物带在头盔上威吓敌人。

刺鲀具有较强的生命力，因此没有出现在世界保护组织的濒危物种清单中。

目录

序

在对超过20000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。在笔者20余年信息系统安全领域的工作经历中，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”。在笔者看来，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，大多数情况下漏洞及其披露缘于系统管理不善、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

不幸的是，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，书中有效地列出了你的敌手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

由于不正确地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（访问）控制

由于不遵守口令策略和不正确的存取控制设置引发的漏洞

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

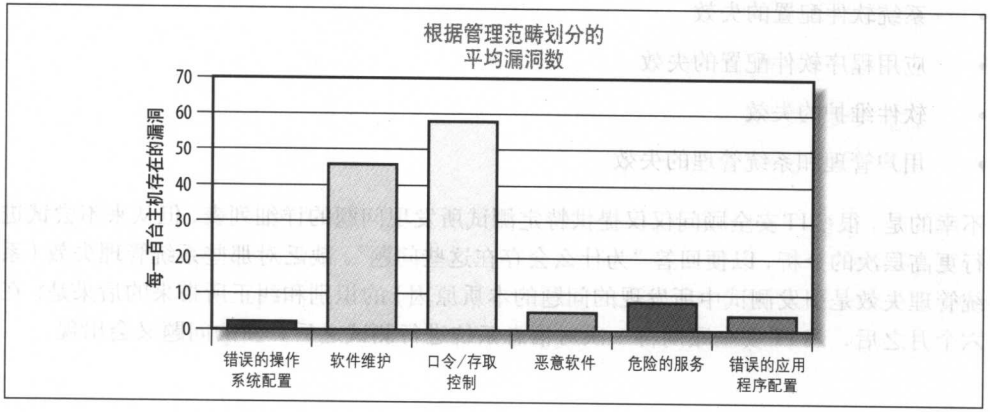
危险的服务

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，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）。

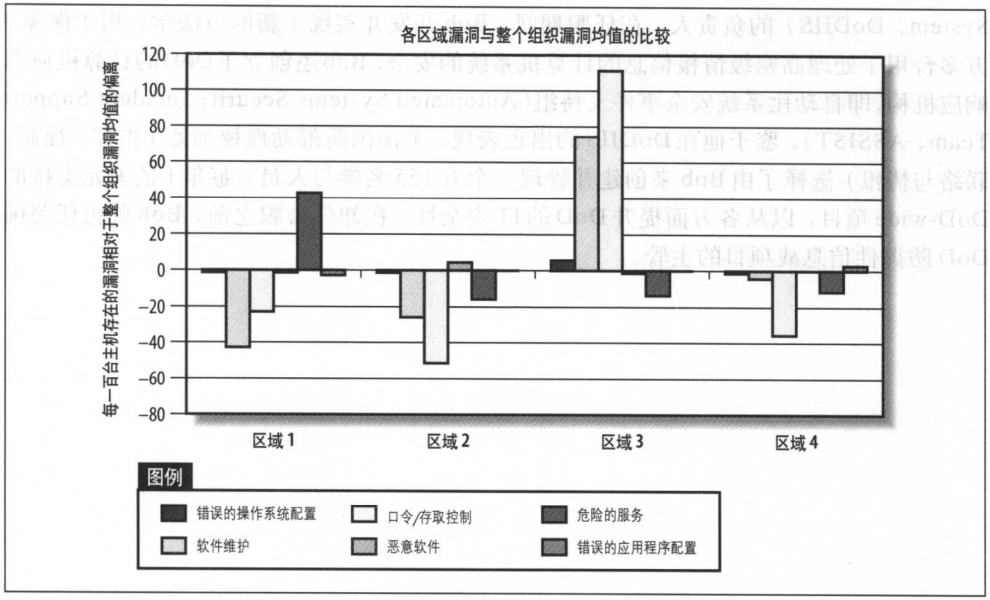


图 F-2：各区域漏洞与整个组织漏洞均值的比较

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注意的重要一点是，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归档了较低层面技术问题的技术报告，但在根本性的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？”

— Bob Ayers

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 安全职位是在美国国防情报局（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4万多台用于处理高密级情报信息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1亿美元支持的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曾担任美国DoD 防御性信息战项目的主管。

前言

对一个黑客而言，闯入一个计算机系统从来就不是绝对不可能的，而只是有时候是不太可能的。

在这样一个信息时代，基于网络的威胁潜伏在每一个角落。在本书写作的时候，无线网络正成为许多公司和组织的痛处——他们不知道该怎样提高其信息基础设施的安全性。网络正面临着来自各种威胁的包围，包括黑客通过Internet进行的攻击、蠕虫、电话盗打以及无线攻击等。

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，以搜索那些易受攻击的组件（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。本书不包含任何与保证你的IP网络安全性无关的其他信息，对于与本书的主题不很相关的那些技术，读者可以从那些可能厚达800页的黑客书籍中去了解。

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，在过去的五年中，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。本书包含了许多检查清单，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。

公认的评估标准

本书基于两个最重要的评估标准，即USA NSA IAM和UK CESG CHECK，这两个标准分别是美国和英国用来测试、保障政府和国家关键基础设施安全性的重要准则。

NSA IAM

美国国家安全局（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：

1. 评估（Assessment）。这一层次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。
2. 评价（Evaluation）。评价是一个协作进行的过程，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。
3. 红队（Red Team）。这一层次的评估是非协作性的，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，诸如BS7799、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进行攻击、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纪录，包括对目标主机相关的DNS纪录结构的正确理解
- 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环境而言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
- 展示如何通过枚举、装配以及操纵NFS导出目录来获取对文件的访问权限
- 检测不安全的X Window服务器
- 展示如何发现并修正如下一些服务中由于配置不当而导致的漏洞：
  - 允许匿名访问的FTP服务
  - 公共的Unix Web服务
  - TFTP服务
  - R服务（包括*rsh*、*rexec*以及*rlogin*）
  - Samba服务
  - SNMP服务

下边给出的则是针对Windows NT环境而言攻击实践课程的参与者所应该具备的一些技术能力：