堆栈攻击
——八层网络安全防御

[美] Michael Gregg
Stephen Watkins
George Mays
Chris Ries
Ron Bandes
Brandon Franklin
著

陈师 译

Hack the Stack
Using Snort and Ethereal to Master the 8 Layers of an Insecure Network

人民邮电出版社
POSTS & TELECOM PRESS

堆栈攻击——八层网络安全防御

[美] Michael Gregg
Stephen Watkins
George Mays
Chris Ries
Ron Bandes
Brandon Franklin
著

陈 师 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

堆栈攻击——八层网络安全防御 /（美）格雷格（Gregg, M.）等著；陈师译. —北京：人民邮电出版社，2008.11
ISBN 978-7-115-18667-6

Ⅰ. 堆… Ⅱ. ①格…②陈… Ⅲ. 计算机网络—安全技术
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 124171 号

版 权 声 明

堆栈攻击——八层网络安全防御

◆ 著 [美] Michael Gregg Stephen Watkins George Mays Chris Ries Ron Bandes Brandon Franklin
译 陈 师
责任编辑 李 际
执行编辑 刘映欣

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京顺义振华印刷厂印刷

◆ 开本：800×1000 1/16
印张：22.25
字数：483 千字 2008 年 11 月第 1 版
印数：1－4 000 册 2008 年 11 月北京第 1 次印刷
著作权合同登记号 图字：01-2007-5568 号
ISBN 978-7-115-18667-6/TP

定价：45.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书利用著名的开放系统互连（OSI）协议堆栈模型，以独特而新颖的观点看待网络安全，将这一综合性的大课题细分到了OSI模型中的每个独立层次当中。作者从分析网络每一层的漏洞出发，假想攻击这些漏洞的各种可能性，在此基础上讨论各个网络层次的安全防御手段。

在讨论了所有的技术环节之后，作者并没有忘记“人”对于网络安全因素的影响，因此在OSI七层模型的基础上扩展了“人工层”。人的行为不像机器那样具有一致性，这增加了防御的难度，然而作者还是根据多年的行业经验为人工层的防御工作指明了方向。

本书的作者都是具有多年行业实践经验的工程专家，他们的背景决定了本书的两大特点：严谨性和实践性。作者的知识层面决定了本书更像是一本具有实践指导作用的工具书籍。本书可谓是网络安全专家以及网络安全行业从业人员的良师益友，而书中提出的类似“安全深度”等思维模式和方法论，值得所有系统工程师借鉴。

序

很多人听到“Hack”一词，首先联想到的就是某种充满恶意的活动。而我则是从一个更广义的角度上去理解它。诚然，不可避免某些Hack行为是恶意的，然而很多却不是。这些非恶意的Hack行为是为了更深层次地探究可编程系统的细节及其真实的工作原理。这些探究行为通常由那些想要了解系统每时每刻工作细节的人发起，目的是为了将系统的能力拓宽到其本身原始设计目标之外的领域。这些非恶意的骇客（Hacker）不同于那些仅想通过学习最有限的知识而达到目的的“脚本小丑”。本书正是为那些寻求更好地理解TCP/IP系统并渴望获得对该系统工作原理更深层次知识的人而作。

本书第1章就向读者提出了将OSI（开放系统互连）体系延伸到网络安全领域的方法。在接下来的章节中，将依次逐层地剥开OSI体系的洋葱皮，其中包括有关第八层——人工层的章节（众所周知，经典的OSI体系只有7个层次）。在附录中对全书作了总结，介绍如何减小被恶意攻击的风险。

谈到该书的写作过程，全赖有George Mays、Stephen Watkins、Chris Ries、Ron Bandes以及 Brandon Franklin等专业人士的帮助，才使得本书得以面世。编纂此书就像一项艰巨的任务，花费了大量的时间，因此我非常感谢他们从紧凑的日常工作中抽出时间和精力来帮助撰写本书。当我多次圆满完成这种艰巨任务的时候，我的朋友和家人总是不断地问，我是如何做到既不耽误工作，又能旅行，还要留出时间进行写作的。嗯，其实秘密只有两个：时间管理和渴望完成任务的心情，就如同Dale Carnegie所说，“如果你坚信所做工作的意义，那么不要让任何事情阻止你去完成它。世界上最好的作品通常就是一些看上去不可能的事物，而关键就是去把它们变成可能。”

我希望本书能够成为你在工作中挑战不可能任务的动力。

——Michael Gregg
Superior Solutions公司CTO

致　谢

Syngress 向以下人员表示感谢，在他们的努力和支持下才有了本书的出版。

当前Syngress书籍由O'Reilly Media公司向美国和加拿大发行。O'Reilly这家企业具有令人惊讶的工作热情和职业素养，我们要感谢那里的每个人，是他们花费了大量的时间和精力，让Syngress书籍进入市场，他们是：Tim O'Reilly、Laura Baldwin、Mark Brokering、Mike Leonard、Donna Selenko、Bonnie Sheehan、Cindy Davis、Grant Kikkert、Opol Matsutaro、Steve Hazelwood、Mark Wilson、Rick Brown、Tim Hinton、Kyle Hart、Sara Winge、Peter Pardo、Leslie Crandell、Regina Aggio Wilkinson、Pascal Honscher、Preston Paull、Susan Thompson、Bruce Stewart、Laura Schmier、Sue Willing、Mark Jacobsen、Betsy Waliszewski、Kathryn Barrett、John Chodacki、Rob Bullington、Kerry Beck、Karen Montgomery以及Patrick Dirden。

我们还要感谢Elsevier Science公司的团队，他们努力让我们的书籍能够面向全世界，团队的成员包括：Jonathan Bunkell、Ian Seager、Duncan Enright、David Burton、Rosanna Ramacciotti、Robert Fairbrother、Miguel Sanchez、Klaus Beran、Emma Wyatt、Krista Leppiko、Marcel Koppes、Judy Chappell、Radek Janousek、Rosie Moss、David Lockley、Nicola Haden、Bill Kennedy、Martina Morris、Kai Wuerfl-Davidek、Christiane Leipersberger、Yvonne Grueneklee、Nadia Balavoine以及Chris Reinders。

同时我们感谢Pansing Distributors发行公司的David Buckland、Marie Chieng、Lucy Chong、Leslie Lim、Audrey Gan、Pang Ai Hua、Joseph Chan、June Lim以及Siti Zuraidah Ahmad，对于我们书籍的热情。

感谢Woodslane发行公司的David Scott、Tricia Wilden、Marilla Burgess、Annette Scott、Andrew Swaffer、Stephen O'Donoghue、Bec Lowe、Mark Langley以及Anyo Geddes，是他们将我们的书籍带入了澳大利亚、新西兰、巴布亚新几内亚、斐济、汤加、所罗门群岛以及库克群岛。

主　　编

Michael Gregg 是 Superior Solutions 公司的总裁，在 IT 领域具有二十多年的经验。他拥有两个专科学位、一个学士学位及一个硕士学位，并且拥有 CISSP、MCSE、MCT、CTT+、A+、N+、Security+、CAN、CCNA、CIW 安全分析师、CCE、CEH、CHFI、CEI、DCNP、ES Dragon IDS、高级 ES Dragon IDS 以及 TICSA 认证。

Michael的主要职责是作为安全项目经理帮助企业以及政府机关保护它们的IT资源和设备。Michael已经出版了4部著作，包括*Inside Network Security Assessment*、*CISSP Prep Questions*、*CISSP Exam Cram2*以及*Certified Ethical Hacker Exam Prep2*。他开发了4门高级安全课程，包括“高级安全全面知识启动集中营”、“Intense School的专业骇客实验指导”、“ASPE的网络安全要素”以及“评估网络漏洞”。他还在网络和各个期刊上发表了专业论文五十多篇，这些期刊和网站包括Certification Magazine、GoCertify、The El Paso Times以及SearchSecurity，等等。

Michael 是 Villanova 大学的教师，也是 Villanova 学院级安全课程的创建者，这些课程包括“信息系统安全要素”、“掌握信息系统安全”以及“高级安全管理”。他还是 4 个 TechTarget 网站的驻站专家，这些网站是 SearchNetworking、SearchSecurity、SearchMobileNetworking 以及 SearchSmallBiz。他还是 TechTarget 编辑委员会的成员。

主要作者

Ronald T. Bandes（CISSP、CCNA、MCSE、Security+）是一位独立安全顾问。在成为独立顾问之前，他负责多家财富 100 强公司，例如 JP Morgan、Dun and Bradstreet 以及 EDS 等的安全工作。Ron 拥有计算机科学专业的学士学位。

Brandon Franklin（GCIA、MCSA、Security+）是 KIT Sloutions 公司的网络管理员。KIT Solutons（KIT 的意思是基于信息技术的知识，Knowledge Based Information Technology）为

卫生与民政部门创建了智能系统，该系统监控并评估影响和工作成果，并且为改进决策提供资源信息。KIT 系统为决策人员、政府机构、私人基金、研究人员以及领域实践人员提供最佳实践建议和基于科学的流程，并演示效果和持续改进结果。

Brandon 曾经是 VigilantMinds 的系统入侵分析团队的领队，VigilantMinds 是一家管理安全服务供应商，总部位于匹兹堡。

Brandon 辅助撰写了第 3 章，并独立撰写了第 6 章。

George Mays（CISSP、CCNA、A+、Network+、Security+、INet+）是一位独立安全顾问，他在计算、数据通信以及网络安全领域具有35年行业经验。他拥有系统分析专业的学士学位。他还是IEEE、CompTIA以及Internet安全等组织的会员。

Chris Ries 是 VigilantMinds 公司（总部位于匹兹堡的管理安全服务供应商和专业顾问机构）的安全研究工程师。他的研究领域是发掘、利用并补救软件中存在的漏洞，分析恶意代码，以及对安全软件进行评估。Chris 基于他的研究发表了一系列技术和顾问白皮书，并对多本信息安全著作做出贡献。

Chris 拥有计算机科学专业的学士学位，并在 Colby 学院辅修了数学专业，在此学习期间他完成了有关恶意代码自动检查的研究。

Chris 还曾经是“国家计算机辩论和培训联盟”（NCFTA）的分析员，在此期间他进行了支持法律执行的技术研究。

Chris 撰写了第 8 章。

技术编辑

Stephen Watkins（CISSP）是一位具有 10 年相关技术经验的信息安全专家，其中 8 年投身于安全领域。他现在是南弗吉尼亚州 Regent 大学的信息保障分析员。在此之前，他带领一个安全专家小组为一个全球性的政府网络提供深度安全分析。最近 8 年，Stephen 在边界安全性和多层安全构架领域积累了大量专业经验。早在 1998 年，Stephen 接触第一代防火墙版本 3.0b 时就对“检查点”技术有所研究了。他在多米尼恩大学获得了计算机学士学位，在詹姆斯·梅迪森大学获得了信息安全方向的计算机硕士学位。他长期居住于弗吉尼亚海滩，他和他的家族热衷于教会和本地的小团体活动。

Stephen 撰写了第 7 章。

目　录

第1章
扩展OSI体系到网络安全领域

1.1 简介

“温故而知新”，本章的目的就是以一种全新的方式将著名的OSI模型应用到当前的安全性话题。后续章节分别侧重于OSI模型的每一个层次，本章则为全书的内容提供一个全局视点。

1.2 阅读指南

本书汇集了安全专家在日常工作中经常要考虑和关注的各种安全性问题。我们将仔细解读一些常见的攻击模式并分析它们是如何成功的。很多攻击之所以能够成功，是因为协议设计较差，而其他的则是程序设计低劣以及编码时缺乏长远考虑所导致。最后将讨论一些用于定位和分析漏洞的非常有用的工具，这些工具被一次又一次地反复使用。

很多书中讨论到的工具，既可以被安全专家使用，也可以被骇客（hacker）利用。当使用这些工具的时候，请确保得到网络所有者的许可，这样可以避免遇到很多令人头疼的问题，或是卷入潜在的法律纠纷。

1.2.1 行业工具

接下来将讨论的协议分析器和入侵检测系统（IDSes）是贯穿本书的两个主要工具。

1. 协议分析器

协议分析器（或嗅探器）是一种非常强大的程序，通过将系统的网卡设置为混杂模式，以接受来自其所处的网络冲突域的所有数据。当网络中使用传统集线器（Hub）时通常执行

被动嗅探。Hub 的使用让数据流向所有端口，这样安全专家或攻击者所要做的就是开启嗅探器，并等着接收同一冲突域内用户所传送的数据。冲突域是一个网络共享的网络片段，但却没有被桥接或交换连接，数据包之间相互冲突是由于所有用户共享同一个带宽导致的。

在交换网络中执行的嗅探叫做主动嗅探，由于它交换来自各个网络片段的数据，因此能够准确知道数据流入的端口。当然这样就增加了对性能的要求。如果试图嗅探所有的交换端口，还可能导致网络堵塞，克服这一缺陷的一个方法是让交换机为每个端口配置一个镜像端口。当然攻击者是没有能力这样做的，因此他们绕过交换功能的最好的机会是毒化和洪泛（这两个概念将在接下来的章节中讨论）。

嗅探器工作于 OSI 模型的数据链路层，这意味着它无需遵循处于堆栈上层的应用程序和服务所要遵循的特定规则。嗅探器能够抓住并保存所有来自电缆上的信息，以便以后分析使用，他们使得用户可以看见所有包含于数据包中的信息。虽然嗅探器对于攻击者来说也是一件非常有效的工具，然而，随着人们越来越多地使用加密技术，它们的效果也大大降低了。

本书中将要使用的嗅探器叫做 Ethereal，这是一种可以同时应用于 Windows 和 Linux 环境的免费工具（第 3 章将更深入讨论如何安装和使用 Ethereal）。如果你已经迫不及待地要使用 Ethereal，那么可以去网站 http://www.ethereal.com了解更多有关它的信息（Ethereal 已被更名为 Wireshark）。

2. 入侵检测系统

入侵检测系统（IDSes）在保护 IT 基础设施的时候扮演了一个非常重要的角色。入侵检测包括监视网络流量，探测非授权访问系统或资源的企图，并通知相关人员以便他们采取对应措施。使用嗅探器分析漏洞和攻击行为，并使用入侵检测系统构建防御体系是一种强大的组合。本书使用的入侵检测系统是 Snort，它同样适用于 Windows 和 Linux 环境，并得到业界的广泛支持。

入侵检测的历史不长。在 1983 年，Dorothy Denning 博士才开始开发第一个入侵检测系统，该系统被美国政府用来分析政府大型计算机的审计日志。

Snort 是由 Martin Roesch 和 Brian Caswell 开发的免费的入侵检测系统。它是一个轻量级的、基于网络的入侵检测系统，能够安装于 Windows 和 Linux 主机上。尽管核心程序使用的是命令行界面（Command Line Interface，CLI），但是图形用户界面也同样可用。Snort 扮演一种网络嗅探器角色并记录符合预定义签名的网络活动。签名为广泛的网络流量所使用，其中包括因特网协议（IP）、传输控制协议（TCP）、用户数据报协议（UDP）以及因特网控制消息协议（ICMP）。

Snort 包含以下两个基本部分：

- **头部**　定义“行为”的规则；
- **可选项**　定义“预警消息”的规则。

要了解更多有关 Snort 的信息，请访问网站 http://www.snort.org。

1.2.2 本书的结构

本书的内容是根据 OSI 模型的层次来组织的，开发 OSI 模型的目的在于为世界网络提供组织和结构指导。在 1983 年，国际化标准组织（ISO）和国际电报电话咨询委员会（CCITT）通过合并文档开发出了 OSI 模型，这是一个基于特定层次结构的模型，每个层次的数据建立在相邻层次的数据输出之上（请参照文档 ISO 7498）。如今，它被广泛地当做一种指导模型用于描述网络环境中的操作，同时被当做骇客、攻击和防御的教学模型。

OSI 模型是一个协议栈，栈中的底层管理硬件的相关处理，而栈中的顶层管理软件的相关处理。控制信息被设计为在 OSI 模型的 7 个层之间传递。表 1.1 描述了 OSI 模型的 7 个层次。

表 1.1 七层 OSI 模型

层次	层次责任
应用层	应用层支持如文件传输协议（FTP）、Telnet 以及超文本传输协议（HTTP）等
表示层	加密、服务器消息块（SMB）、信息交互美国标准（ASCII）以及格式化
会话层	数据流控制、启始、关闭以及错误检测/恢复
传输层	端对端通信，UDP 和 TCP 服务
网络层	路由和可路由信息，例如 IP 和开放最短路径优先（OSPF）协议，传输的最佳路径和效率控制
数据链路层	网络接口卡、媒体访问控制（MAC）协议地址、帧、格式化和数据组织
物理层	传输介质，例如双绞线、无线系统以及光纤等

OSI 模型的功能如下：

（1）信息从应用层传入一直向下传输直到物理层；

（2）接下来数据通过物理介质（例如，电线、同轴电缆或无线）传到目的设备；

（3）一旦到达目的设备，数据由堆栈的反方向传输到应用层。

在本书中，OSI 模型被加入了第八层，我们称之为人工层（或社会层）。图 1.1 展示了这 8 个层次并解读了各层提供的服务。

OSI 的官方模型是 7 个层次，但为了更好地描述发生在网络环境中的骇客和攻击行为，第八层（人工层）被加入模型中。

1. 人工层

被称为人工层的第八层虽不是 OSI 模型的官方定义层次，却是一个非常值得考虑的重要环节。因此，在本书中它被加入 OSI 模型中。人工层往往是最薄弱的环节。企业能够在七层的 OSI 模型上构建出最好的防御方案，却往往因为人工或雇员的因素受到安全威胁。社交工程、网络钓鱼、电话线路盗用以及垃圾数据挖掘等都是经常采用的攻击手段。

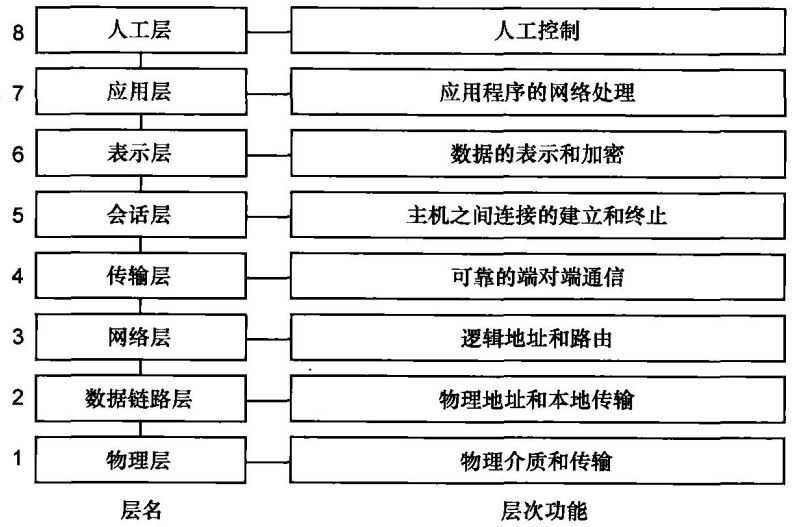

图 1.1　堆栈攻击的八层

内幕信息

早期的电话线路盗用

电话系统骇客（或称为电话线路盗用）比计算机骇客更早出现。盗用者通过各种技术来操控电话系统以达到免费打电话的目的。一种叫做“蓝盒”的早期技术通过复制用于长途电话交换的电频音来实现目的。当年，电话公司使用同一条线路来做语音通信的交换。蓝盒之所以得名是由于这种非法设备首次被电话公司发现的时候是装在一个蓝色塑料盒中。蓝盒的一个关键能力是它能够发出一个 2600Hz 的电频音，该电频音能够绕过电话公司的记账系统而使用户可以免费拨打长途电话。即便是盗用者无法制造出蓝盒，电话公司也不见得就安全了。在 20 世纪 70 年代的早期，有人发现在玩具口哨中放入爆米花能够产生同样频率的声波。任何人都可以用这种口哨来发送信令，从而免费拨打通向世界各地的长途电话。

2. 应用层

第七层被称为应用层。被认为是官方 OSI 模型的最顶层，作为应用服务程序通向网络的窗口。第七层不是一个真正的应用程序，而是一个应用程序之间的通信渠道。

3. 表示层

第六层被称为表示层。表示层最主要的目的就是定义数据表现的格式，并向应用层提交数据。这些数据必须被正确地格式化，这样应用层才能够正确地理解和解析。以下几条是表示层的责任：

- 加密和解密消息；
- 压缩和解压缩消息，并将其格式化；

- 处理协议之间的转换。

4. 会话层

第五层为会话层，其目的是允许不同计算机的应用程序之间建立并维护一段会话。同时它还负责在信息和数据被移动的时候通知该段会话，当数据传输完毕之后，该段会话将被终止。会话层协议包括：

- 远程过程调用（RPC）；
- 结构化查询语言（SQL）。

5. 传输层

第四层为传输层。应用层、表示层、会话层主要关心的对象是数据，而传输层所关注的是数据片段。根据应用协议的不同，传输层可以选择快速地或是可靠地传输信息。传输层的责任包括端对端的错误恢复和流量控制。该层中最常用的两大协议为：

- **传输控制协议** 一种面向连接的协议，通过使用握手、认证、错误检测以及会话终止等手段提供可靠的数据通信；
- **用户数据报协议** 一种无连接的协议，高速和低开销是其两大主要优势。

6. 网络层

第三层是网络层。该层主要还是软件处理，处理对象是数据包。网络层是 IP 的家，IP 在数据发布以及在数据源和数据目的之间寻求最佳传输路径方面起到重要的作用。网络层的组件包括：

- 路由器；
- 无状态检测/数据包过滤。

7. 数据链路层

第二层是数据链路层。该层主要处理单个局域网（LAN）之间的数据流。数据链路层在将数据传送给物理层之间会对数据进行组织和格式化。由于其自身的物理性特点，该层主要使用硬编码的媒体访问控制（MAC）协议地址。数据链路层将数据单位切分为数据帧。当数据帧到达目的设备时，数据链路层将剥掉数据帧的帧头，而将剩下的数据包传递给网络层。数据链路层的组件包括：

- 桥；
- 交换机；
- 网络接口卡（NIC）；
- MAC 地址。

8. 物理层

OSI 模型的第一层就是物理层。电频比特传输就发生在这一层。在电线上传输的比特不具备任何实际意义，然而物理层却定义了比特的持续时间以及发送接收方式。物理层的组件包括铜缆、光缆、无线系统组件以及以太网集线器。在本书中，物理层还被扩展到以下方面：