

# 《堆栈攻击》

## 图书基本信息

书名：《堆栈攻击》

13位ISBN编号：9787115186676

10位ISBN编号：7115186677

出版时间：2008-11

出版社：人民邮电出版社

页数：344

译者：陈师

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《堆栈攻击》

## 前言

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”。

# 《堆栈攻击》

## 内容概要

《堆栈攻击:八层网络安全防御》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。《堆栈攻击:八层网络安全防御》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《堆栈攻击:八层网络安全防御》的两大特点：严谨性和实践性。作者的知识层面决定了《堆栈攻击:八层网络安全防御》更像是一本具有实践指导作用的工具书籍。《堆栈攻击:八层网络安全防御》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。

# 《堆栈攻击》

## 作者简介

作者：(美国)格雷格 (Michael Gregg) (美国)Stephen Watkins (美国)George Mays 译者：陈师

# 《堆栈攻击》

## 书籍目录

第1章 扩展OSI体系到网络安全领域	1.1 简介	1.2 阅读指南	1.2.1 行业工具
1.2.2 本书的结构	1.3 常见的堆栈攻击	1.3.1 人工层	1.3.2 应用层
1.3.3 会话层	1.3.4 传输层	1.3.5 网络层	1.3.6 数据链路层
1.3.7 物理层	1.4 将OSI模型映射到TCP/IP模型	1.5 IT安全领域的当前状况	1.5.1 物理安全
1.5.2 通信安全	1.5.3 信令安全	1.5.4 计算机安全	1.5.5 网络安全
1.5.6 信息安全	1.6 使用书中的信息	1.6.1 漏洞测试	1.6.2 安全性测试
1.6.3 查找并报告漏洞	1.7 小结	1.8 总结性回顾	1.9 FAQ
第2章 第一层：物理层	2.1 简介	2.2 保护物理层	2.2.1 设计安全
2.2.2 外围安全	2.2.3 建筑设施安全	2.2.4 设备安全	2.2.5 通信安全
2.3 攻击物理层	2.3.1 偷窃数据	2.3.2 撬锁	2.3.3 线路盗窃
2.3.4 扫描和嗅探	2.3.5 硬件攻击	2.4 物理层安全工程	2.5 小结
2.6 总结性回顾	2.7 FAQ	第3章 第二层：数据链路层	3.1 简介
3.2 以太网和数据链路层	3.2.1 以太网数据帧结构	3.2.2 理解MAC寻址	3.2.3 理解以太类别
3.3 理解PPP和SLIP	3.3.1 串行线路网际协议	3.3.2 点对点协议	3.4 使用协议分析器
3.4.1 编写伯克利数据包过滤器	3.4.2 检测实时数据流量	3.4.3 数据流量过滤，第二部分	3.5 地址解析协议的工作原理
3.6 攻击数据链路层	3.6.1 被动嗅探与主动嗅探	3.6.2 ARP毒化	3.6.3 ARP洪泛
3.6.4 路由游戏	3.6.5 嗅探无线网络	3.6.6 无线网络的受攻击点	3.7 保护数据链路层
3.8 抵御嗅探器的安全措施	3.8.1 使用加密措施	3.8.2 安全套接字层	3.8.3 非常保密机制和安全/多用途网际邮件扩展协议
3.8.4 交换技术	3.9 应用侦测技术	3.9.1 本地侦测	3.9.2 网络侦测
3.10 数据链路层安全工程	3.11 小结	3.12 总结性回顾	3.13 FAQ
第4章 第三层：网络层	4.1 简介	4.2 IP数据包结构	4.2.1 鉴别IP的版本
4.2.2 服务类别	4.2.3 总长度	4.2.4 数据报身份识别码	4.2.5 分组
4.2.6 生命周期	4.2.7 协议字段	4.2.8 检测码	4.2.9 IP地址
4.2.10 IP选项字段	4.3 ICMP数据包结构	4.3.1 ICMP基础知识	4.3.2 ICMP消息类别以及格式
4.3.3 常见的ICMP消息	4.4 攻击网络层	4.4.1 IP攻击	4.4.2 ICMP攻击
4.4.3 路由器和路由攻击	4.5 保护网络层	4.5.1 加强IP的安全性	4.5.2 加强ICMP的安全性
4.5.3 加强路由器和路由协议的安全性	4.6 网络层安全工程	4.6.1 Pttunnel	4.6.2 ACKCMD
4.7 小结	4.8 总结性回顾	4.9 FAQ	第5章 第四层：传输层
5.1 简介	5.2 面向连接协议与无连接协议	5.2.1 面向连接协议	5.2.2 无连接协议
5.2.3 为什么会同时具有这两种协议	5.3 位于传输层的协议	5.3.1 UDP	5.3.2 TCP
5.3.3 TCP会话的开始和结束	5.4 骇客的视角	5.5 扫描网络	5.5.1 端口扫描概述
5.5.2 TCP扫描的各种花样	5.5.3 Nmap基础	5.6 操作系统指纹识别	5.6.1 操作系统探测的工作过程
5.6.2 Xprobe 2	5.6.3 使用Nmap进行操作系统指纹识别	5.7 侦测对网络的扫描	5.7.1 Snort的规则
5.7.2 Snort用户接口——基本分析和安全引擎	5.8 保护传输层	5.8.1 SSL协议的工作过程	5.8.2 SSL在网络中的表现形式
5.8.3 SSL/TLS总结	5.9 传输层工程——建立Snort系统	5.9.1 开始旅程	5.9.2 安装Fedora Core 4
5.9.3 安装支持软件	5.10 小结	5.11 总结性回顾	5.12 FAQ
第6章 第五层：会话层	6.1 简介	6.2 攻击会话层	6.2.1 观察SYN攻击
6.2.2 会话劫持	6.2.3 嗅探会话建立过程	6.2.4 认证	6.2.5 观察RST攻击
6.2.6 在会话层挫败Snort系统	6.3 保护会话层	6.3.1 减轻DoS攻击	6.3.2 防止会话劫持
6.3.3 选择认证协议	6.3.4 抵御RST攻击	6.3.5 侦测会话层的攻击	6.3.6 端口敲击
6.4 会话层安全工程	6.5 小结	6.6 总结性回顾	6.7 FAQ
第7章 第六层：表示层	7.1 简介	7.2 NetBIOS和SMB的结构	7.3 攻击表示层
7.3.1 NetBIOS和枚举	7.3.2 嗅探加密数据流	7.4 保护表示层	7.4.1 加密
7.4.2 IPsec的角色	7.4.3 保护电子邮件	7.4.4 加强NetBIOS保护	7.5 表示层安全工程
7.6 小结	7.7 总结性回顾	7.8 FAQ	7.9 参考文献
第8章 第七层：应用层	8.1 简介	8.2 FTP的结构	8.2.1 FTP概述
8.2.2 FTP实例	8.2.3 FTP安全问题	8.3 分析域名系统及其弱点	8.3.1 域名消息格式

# 《堆栈攻击》

8.3.2 DNS查询过程	8.3.3 DNS层次	8.3.4 缓存	8.3.5 分区和分区传输
8.3.6 DNS工具	8.3.7 DNS安全问题	8.4 其他非安全的应用层协议	8.4.1 简单邮件传输协议
8.4.2 Telnet	8.4.3 其他协议	8.5 攻击应用层	8.5.1 攻击Web应用程序
8.5.2 攻击DNS	8.5.3 缓存溢出	8.5.4 逆向工程代码	8.5.5 应用攻击平台
8.6 保护应用层	8.6.1 SSH	8.6.2 非常保密机制	8.6.3 安全化软件
8.6.4 加固系统	8.6.5 漏洞扫描器	8.7 Nessus	8.8 应用层安全工程：使用Nessus来安全化堆栈
8.9 小结	8.10 总结性回顾	8.11 FAQ	第9章 第八层：人工层
9.1 简介	9.2 攻击人工层	9.2.1 社会工程	9.2.2 盗用电话线路
9.2.3 万维网、电子邮件以及即时消息	9.3 保护人工层	9.3.1 政策、流程以及指导方针	9.3.2 人对人认证
9.3.3 数据分类和处理	9.3.4 教育、培训以及意识规划	9.3.5 测试	9.3.6 监控和执行
9.3.7 定期更新评测和控制	9.3.8 法规要求	9.4 如何加强安全性	9.5 人工层安全工程
9.6 小结	9.7 总结性回顾	9.8 FAQ	附录A 降低风险：加强协议栈的安全性
A.1 简介	A.2 物理层	A.3 数据链路层	A.4 网络层
A.5 传输层	A.6 会话层	A.7 表示层	A.8 应用层
A.9 人工层	A.10 小结		

# 《堆栈攻击》

## 章节摘录

插图：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。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

# 《堆栈攻击》

## 编辑推荐

《堆栈攻击:八层网络安全防御》正是为那些寻求更好地理解TCP / IP系统并渴望获得关于该系统工作原理更深层次知识的人而作。凭借这些知识。安全专家能够让网络更加安全。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。诚然。不可避免有些Hack行为是恶意的，然而很多则不是。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。



# 《堆栈攻击》

## 精彩短评

- 1、随手翻了一下，这书好imba，第二章就教人如何开挂锁
- 2、稍微有点基础的新手也能看懂，而且生动。缺点是个别章节写的很拗口，结构有些散乱，有些重复的地方。理论不扎实的可能需要另买一本教科书类型的来补充一下。
- 3、东西都没问题，包装也很好，是个很安全的硬纸盒子包装。
- 4、这本书在新华书店看了很久，觉得没有某些书好，不过闲钱多的话买来看看还是有好处的
- 5、用啃的
- 6、概括上的简介，需要自己更深入的去学习
- 7、难得有本讲原理的好书啊
- 8、网络安全方面入门初级读物，不要有太多期望了。
- 9、叙述手法比较特别，但是由于从1层写到了8层，则不可避免的造成每一章的内容都是点到为止

## 《堆栈攻击》

### 精彩书评

1、自己的行当几乎是网络安全了，每每走图书馆的网络安全书架旁边我却都快步走过去，简直是羞于被人发现看《黑客秘籍...》，《黑客。。。》之类的书籍，一方面是别人认认自己是还在幻想黑客的年龄，另一方面是那些书籍确实是垃圾，教一点儿工具的使用都以为是在传道授业解惑，简直是侮辱了这个行业。反而是想找一本真真的能讲这方面技术的书籍很难，刚走出了教人用工具的路子又是走进了全篇理论的怪圈。这本书图不同在于此，以一个安全从业人员的角度讲解了进行攻击的方式，同时再讨论了怎样预防这些工具，总体来说，是一本不错的入门书籍。ps: 这书开篇就教人撬锁，有此工作意向的人可以看一下，当然，也只是入门！

## 章节试读

### 1、《堆栈攻击》的笔记-第321页

风险是不可能被彻底消除的，它只能被减少或处理。通过避免，专家或减轻等手段之后，任何还存在的风险叫做“剩余风险”。

# 《堆栈攻击》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)