《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

《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

《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，一方面是别人认认为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！

《堆栈攻击》

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