<<网络安全HACKS>>

图书基本信息

书名：<<网络安全HACKS>>

13位ISBN编号：9787508392790

10位ISBN编号：7508392795

出版时间：2010-3

出版时间：中国电力出版社

作者：洛克哈特

页数：452

译者：陈新

前言

在网络安全领域，人们常常会误解黑客这个词的意思。
这是可以理解的，因为网络安全专家会使用工具来探测自身网络的稳健性，然而攻击者也可以用这些工具实施对因特网上主机的攻击。
系统管理员合法地测试自己的机器，而系统破坏者则试图获得未授权的访问权限。
他们在技术上和使用工具方面并没有什么不同，但是他们的意图却完全不同。
毕竟，和任何强大的技术一样，没有一个安全工具天生是正义的或恶意的——这完全取决于如何使用该工具。
同一个锤头可以用来建造城墙，也可以用来推倒城墙。
“白帽子”黑客和“黑帽子”黑客的区别并不在于他们所使用的工具或技术（甚至是他们帽子的颜色），而是在于他们的意图。
这样的区别很微妙，但是却十分重要。
白帽子黑客将构建安全的系统作为一项有趣的挑战，并且希望构建的系统的安全性可以彻底通过真实环境下的测试（假定该环境下攻击者拥有所有破坏系统的技术和工具）。
黑帽子黑客（更合适的称呼是骇客）学习和白帽子黑客相同的技术，但是对构建系统的人员及他们攻击的服务器并不关心。
黑帽子黑客使用自己的技术来破坏这些系统，从而获得自己个人的收益，他们经常破坏被他们渗透的系统。
当然，国际上有一些大胆的依靠技术“抢劫”的人以及一袭黑衣、叼着香烟、挥舞着笔记本的邪恶的计算机天才，他们的故事往往比单纯构建一个健壮网络的工程师的故事受人们欢迎，因此，“hacking”这个词在媒体中享有的声誉比较差。
媒体通常将黑客看做是那些闯入系统或用计算机作为武器来发起破坏行为的人。
然而那些解决计算机实际问题的人们通常将“hack”这个词看做是快速解决某个问题，或者是一个完成某件事情的巧妙的方法。

<<网络安全HACKS>>

内容概要

入侵者用于网络攻击的技术在发展，因此用于保护自己和网络的工具和方法也必须及时修改以跟上步伐。
本书更新了所有系统关键的工具，并为两年前不存在的问题提供了灵活的解决方案。
新版本展示了如何检测网络入侵者的存在，使用强加密保护网络和数据，甚至要为可能的系统破坏者设下埋伏。
相比以前的版本，新版本更大、更广泛，并更具有实用性，它陈述了125个真实世界的工具和技巧，专家就是用这些手段来加强他们对攻击者的防护。
在本书中，您将看到一些很有用的检测并处理入侵者的技术，学到以下内容：　　· 通过躲避网络流量分析和加密电子邮件来保护隐私。
· 通过captive portal(强制网络门户)共享无线网络，使用良好粒度的鉴别来保护无线网络。
· 建立看起来容易遭受攻击的虚拟网络(蜜罐)，来转移攻击者注意力，或者迷惑攻击者。
· 加强Linux、BSD和Windows主机安全，防范攻击。
· 使用先进的入侵检测系统监视网络和服务。
· 使用强VPN解决方案通过互联网安全地连接两个远程站点。
· 检测系统漏洞，当系统遭受攻击时如何进行响应和恢复。
要获取更有效的安全工具，需要学习攻击者使用的最新技术。
本书提供了维持网络安全可靠所需的信息。

作者简介

作者:(美国) 洛克哈特

<<网络安全HACKS>>

书籍目录

章节摘录

插图：因为联网就是将计算机连在一起，所以计算机网络的安全性不会大于连接在该网络中计算机的安全性。
单个不安全的主机会给整个网络带来许多不安全因素，因为在敌方控制下，可以利用其作为一个侦察工具或一个强大的攻击堡垒。
如果服务器提供容易危及服务器安全的服务，那么即使采用防火墙、入侵检测系统和其他高级安全措施也是没有用的。
因此在深入研究网络部分的安全前，应该首先确保自己所负责区域中的计算机是尽可能安全的。
本章提供很多方法来减少在基于unix系统上提供服务所带来的风险。
尽管每个小节各自独立，还是很值得通读本章内容的。
因为如果仅仅实现一种类型的安全措施，将面临着一旦攻击者发现如何绕过所应用的安全措施，所有的准备工作将被完全否定的风险。
正如不会只使用一个普通的门和插销来保护诺克斯堡（译者注）一样，没有哪种单一的安全方法能从根本上保护您的服务器。
并且，需要采用的安全措施是与被保护对象的自身价值成正比的。
俗话讲：“安全不是名词，安全是动词”。
这就是说，安全是一个活动的过程，它必须得到不断的跟踪和更新。
除了断开计算机的网络连接外，没有哪种单一的方法能彻底保证计算机安全。
基于这种观点，我们可以将这里所要介绍的技术看做是构建满足特定需求的安全服务器的基础。

编辑推荐

《网络安全Hacks(第2版)》由中国电力出版社出版。

版权说明