<<黑客札记>>

图书基本信息

书名：<<黑客札记>>

13位ISBN编号：9787302087519

10位ISBN编号：7302087512

出版时间：2004-7-1

出版时间：清华大学出版社

作者：杨战伟,李颖利,Nitesh Dhanjani

页数：226

字数：241

译者：杨战伟,李颖利

<<黑客札记>>

内容概要

本书将告诉你黑客如何思考，以使你能够找到办法保护Unix和Linux系统不受他们攻击。
这是可以知道如何阻止系统被入侵的惟一方法。
为了阻止最有经验的黑客攻击，我们需要了解他们的思考过程、技术和策略。
Unix和Linux操作系统功能强大的本质是一把双刃剑。
在大多数情况下，操作系统内核源码是可以免费得到的，管理员可以对内核做很大的变动以满足自己的需要。
但是Unix和Linux这个功能强大和灵活的本质包含很多的复杂性，增加了可以轻易使系统处于危险的错误配置的几率。
我们还要考虑目前可用的Unix和Linux发布版本的不同。
每个版本都绑定它自己的一套安全策略和配置。
例如，一些发布版本关闭了一组远程服务，而另外一些则开启了所有可能的服务，而安全策略最为薄弱。
黑客意识到管理Unix和Linux主机的复杂性，并且确切地知道该如何利用它们。
本书中介绍的最巧妙的黑客策略将会使你大吃一惊，本书还会教你如何防御这些黑客攻击。

不要担心黑客会掌握本书中提供的资料，因为他们早已经了解了这些内容。
本书的目的是披露目前黑客使用的攻击策略，因此可以学习如何对付他们。
一旦知道黑客的思考方式和他们用于侵入系统的多种不同的方法，形势就对我们有利了。

本书的组织形式
本书分为四个主要部分：
第一部分：黑客入侵技术及防御
本书的第一部分讲述了黑客目前普遍使用的入侵技术还介绍了针对这些章节中描述的所有入侵技术的防御技术。
第1章 我们从理解入侵技术的第一个逻辑步骤开始：追踪。
本章将告诉你黑客如何通过搜索引擎、注册记录、DNS记录及更多渠道获取公共的可用信息。
一旦从公共可用资源获得所有可得信息后，他们会开始进行实际的网络及主机的辨识和扫描。
第2章 本章告诉你如何判断网络中的哪一台主机是运行的，以及它们开放的端口。
我们会讨论不同的扫描端口的方法，同时讨论的还有操作系统辨识技术和工具。

第3章 学习黑客如何辨识运行在远端主机上的应用程序和服务。
本章将介绍很多潜在的入侵者枚举用户名和远端服务所用的不同工具和方法。
第4章 本章披露了黑客获得易受攻击主机的访问权限所用的具体工具和策略。
学习黑客使用的最巧妙的技术，比如暴力破解、嗅探、中途攻击、密码破解、端口重定向，以及对配置不当、缓冲区溢出及其他软件系统安全漏洞的利用。

第5章 对特定漏洞的利用通常可使黑客获得无特权用户或系统账户的权限。
在这些情况下，对于黑客来说下一步是获得超级用户(root)权限。
本章展示了黑客试图获得更高级权限而使用的各种不同的方法。
第6章 一旦某个主机被入侵，黑客希望隐藏他的存在并确保对主机的持续且有特权的访问。
本章告诉你黑客们如何通过清空重要日志以隐藏他们的痕迹以及黑客如何给入侵目标主机安装特洛伊木马、后门和rootkit攻击工具。
第二部分：主机安全强化
本书的第二部分集中讲述了系统管理员可能采用的强化默认系统配置和策略的多个步骤。

第7章 本章讨论了与强化默认应用程序和服务器配置相关的重要配置问题。
我们鼓励所有的系统管理员都考虑一下本章的建议以阻止入侵者攻击薄弱的系统策略和配置。

第8章 恶意用户和黑客经常利用那些不适当的用户和文件系统许可,本章将介绍UNIX和LINUX文件许可,并且讲述了抵御由于不良用户和文件许可而造成的入侵所采取的确切步骤.
第9章 每个系统管理员都应该执行正确的系统事件日志记录。
本章教给你如何开启和配置有用的日志记录服务，以及如何在日志文件中正确地设置许可以防止它们被篡改。
及时下载最新的安全补丁也是很重要的，本章提供了可获得这些信息的官方网址的有用链接。
第三部分：专题
本书的第三部分围绕几个令人兴奋的话题展开，包括为Nessus扫描器编写插件程序、无线入侵，以及利用ZaurusPDA的入侵。
第10章 Nessus是一个目前最流行的漏洞扫描工具。
它是免费的并且设计成模块化形式。
本章教给你如何使用NASL(Nessus攻击脚本语言)为Nessus扫描器编写定制的安全漏洞检查插件程序。
第11章 学习黑客如何侵入802．11无线网络。
本章叙述了WEP协议的薄弱环节，并介绍了黑客人侵无线网络所使用的工具。
另外，本章提出了一些如何更好地保护无线网络的建议。

第12章 夏普的ZaurusPDA设备运行的是嵌入式Linux操作系统。
本章向你展示了用于ZaurusPDA的各种安全工具以及它们是如何轻易地被黑客利用来侵入无线网络的。

参考中心 这一部分安排在本书的最后以便于查询。
当我们需要获得关于常用命令、常用端口、在线资源、IP地址，及有用的Netcat命令之类问题的快速信息时，记得把书翻到这一部分。
另外，这一部分还提供ASCII值和HTTP响应表。
写给读者的话
作者对本书的编写做出了很多努力。
希望读者能够在书中找到有价值的资料。
最重要的是，希望读者把本书中提供的信息用于保护自己的系统和网络不被最有经验的黑客人侵。

作者简介

Nitesh Dhanjani是Foundstone公司的一位信息安全顾问。
他参与编写了一本最畅销的关于计算机安全性的书籍《黑客大曝光》以及《黑客杞记网络安全手册》
。
他已经为财富500强企业中的许多客户进行了网络及Web应用程序攻击和渗透检查。

丛书编辑介绍：Mike Horton是Fou

<<黑客札记>>

书籍目录

版权说明