《反黑客工具箱》

图书基本信息

书名：《反黑客工具箱》

13位ISBN编号：9787302188704

10位ISBN编号：730218870X

出版时间：2009-1

出版社：清华大学出版社

页数：672

译者：余杰,黄彩霞

《反黑客工具箱》

前言

在大家眼中，“ 黑客 ”一词具有一定的神秘性，其定义范围包括了反社会的计算机天才到恶意病毒的编写者。因此，如同在媒体故事中所描述的那样，现代黑客试图攻击网络，从而进行识别偷窃、窃取信用卡账号、勒索银行或者发起拒绝服务攻击等。然而，黑客也可能是那些非常有天分的程序员，他们将众多强大的工具组合起来解决自己的需求，还可能是那些使用“ 合法的 ”工具来绕过审查机构限制并保护个人隐私的人。Internet本身不产生诡计、勒索、偷窃或者镇压——它只是为这些活动提供了途径。当然，Internet的全球分布性和直接通信便捷了黑客的活动。因此，计算机安全——防范黑客——已经成为研究、开发、商业、媒体和市场等领域的一个重要主题。本书将介绍一些工具，这些工具已经成为了计算机和网络安全的一个完整部分。我们希望通过介绍这些工具，读者能够获得如何测试和保护自己的计算环境的知识，同时我们还揭开了黑客的部分神秘面纱。最后，对许多工具及其如何使用进行了摘要介绍。计算机安全是一个处理起来很棘手的问题，因为只要拥有了足够的工具和时间，几乎任何联网设备都可能被利用、扫描或者攻陷。因此，从防御的观点来看，拥有最好的工具来确定周边环境的风险以及实现反击方法是非常重要的。某些工具也许能够完成某项任务，但却不能让整个任务很好地完成。在根据任务选择正确的工具之前，必须了解需要获取哪些工具，必须明白这些工具在主机和网络管理下如何使用，以及它们如何被用来攻击系统。本书的目标是描述使用安全工具的“ 最佳实践 ”，不仅给出如何使用工具的背景还介绍了为什么以及何时使用某款特定工具的深层原因。仅仅知道某款工具的存在及其命令行选项而没有关于该工具的底层安全原理和概念性的理解，在当今是无法专业地维护IT安全的。通过使用截屏、列举代码、工具使用示例和案例分析，本书旨在展现每款工具是如何用于特定真实世界场景中的，这些场景可以折射到读者自己的应用中。尽管对命令行标记和配置选项的包含也使得本书可以成为一款有用的桌面工具，但在每章中包含的附加信息和基本概念使得本书不仅仅是一个“ 如何操作 ”的指南。读者可以根据自己的需要熟悉和掌握工具，因此就可以有效地选择（并使用）正确的工具来很好地完成任务。

《反黑客工具箱》

内容概要

《反黑客工具箱(第3版)》提供了获取最新的网络安全工具的途径，有助于在网络受到攻击并瘫痪后快速地恢复。《反黑客工具箱(第3版)》是以工具的类别为逻辑组织起来的，对每种工具的功能、安装和配置进行了详尽的介绍，同时还提供了使用截屏和代码示例。新颖的示例和深入的案例学习详细地说明了每一种工具在现实世界中的具体应用。

《反黑客工具箱》

作者简介

Mike Shema是NT Objectives公司的CSO（信息安全主管）。他是McGrawHill/Osborne所出版的Hacking Exposed Web Application（WEB应用黑客大曝光，清华大学出版社出版了该书的中文版）的合作作者。

《反黑客工具箱》

书籍目录

《反黑客工具箱》

章节摘录

第 I 部分 多功能工具第1章 Netcat和Cryptcat本书将介绍多种网络安全工具和黑客工具。大多数情况下，一种工具往往用于某一特定目的。例如，有些黑客工具用于收集网络及其内部主机的信息，而另一些工具则直接搜寻易受攻击的系统。然而，最有用和最常用的工具往往是那些具有多种功能，并且可以适用于不同场合的工具，例如Netcat和Cryptcat。1.1 Netcat简单地说，Netcat建立并接受传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）连接。Netcat可在这些连接上读写数据，直到连接关闭为止。它提供了一个基本的TCP／UDP网络子系统，使用户可以手工或者通过脚本与应用层的网络应用程序或服务进行交互。在被文件传输协议（File Transfer Protocol，FTP）、简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）或者超文本传输协议（Hypertext Transfer Protocol，HTTP）等最高层协议封装之前，可以使用该工具查看原始的TCP及UDP数据。注意：从技术上讲，Netcat并不能产生UDP连接，因为UDP是一种无连接的协议。就本章而言，每当谈到使用Netcat建立一个UDP连接时，都是指在UDP模式中使用Netcat向可能运行在接收端的某个UDP服务发送数据。Netcat并不能完成奇特的工作。它没有漂亮的图形用户界面（GUI），也不能输出报告形式的结果。它很粗糙、原始和丑陋，但是由于它在一个非常基础的层次上工作，因此这个工具在许多情况下都很有用。因为Netcat如果不与其他工具和技术进行结合就得不到任何有用的结果，所以没有经验的用户可能认为Netcat只是一个Telnet客户端工具，而另一些用户则可能很难从冗长的Readme文件中看出它是一个强大的工具。但是，读完本章，读者将了解到为什么Netcat会成为工具包中最有用的工具之一。使用现在，许多基于Linux和BSD的操作系统都将Netcat作为系统默认工具包的一部分，甚至Cygwin现在也将Netcat作为安装选项。这是Netcat十分有用的证据之一。如果读者的系统中已经安装了Netcat，或者可以轻易找到用于安装的RPM包，就可以跳过“ 下载 ”一节。注意大多数预装的版本都不支持.e选项（在套接字上执行命令），但是也可以将命令用管道输入其中。因此，如果Netcat不是当前版本或者希望使用其附加的功能，就需要从源代码上下载并安装该工具。

《反黑客工具箱》

编辑推荐

《反黑客工具箱(第3版)》在上一版本的基础上进行了完整更新，最新黑客工具的详细说明，涵盖无线、取证、防病毒、网络钓鱼、网址嫁接等领域。覆盖Windows、Linux/UNIX和Mac OS X。

《反黑客工具箱》

版权说明