安全技术经典译丛

Anti-Hacker Tool Kit Third Edition

反黑客工具箱

(第3版)

(美) Mike Shema
Chris Davis
Aaron Philipp
David Cowen
著

余 杰 黄彩霞 译

- 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

Mc Graw Hill Education

Mc Graw Hill

清华大学出版社

反黑客工具箱

安全技术经典译丛

Anti-Hacker Tool Kit Third Edition

反黑客工具箱（第3版）

(美) Mike Shema
Chris Davis
Aaron Philipp
David Cowen
著

余 杰 黄彩霞 译

清华大学出版社

北 京

Mike Shema、Chris Davis、Aaron Philipp、David Cowen

Anti-Hacker Tool Kit，Third Edition

EISBN: 0-07-226287-7

图书在版编目(CIP)数据

反黑客工具箱(第 3 版)/(美)舍马(Shema,M.)等著；余杰，黄彩霞 译. —北京：清华大学出版社，2009.1
(安全技术经典译丛)

书名原文：Anti-Hacker Tool Kit，Third Edition

ISBN 978-7-302-18870-4

I.反…　II.①舍…　②余…　③黄…　III.计算机网络—安全技术　IV.TP393.08

中国版本图书馆 CIP 数据核字(2008)第 173675 号

责任编辑：王　军　郑雪梅
封面设计：久久度文化
版式设计：康　博
责任校对：胡雁翎
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：42.75　**字　数**：1094 千字
版　　次：2009 年 1 月第 1 版　　**印　　次**：2009 年 1 月第1 次印刷
印　　数：1～4000
定　　价：86.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：027685-01

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。

本书分为 4 个部分：多功能工具、审计与主机防护工具、审计和保护网络的工具以及取证与事件响应的工具。这 4 部分的内容组成了本书，读者可以选择恰当的和特定领域的工具来浏览：

- 审计和防御
- 事件检测
- 调查和响应
- 补救

以上 4 个方面集中体现了系统管理员需要花费大量精力来处理的工作。这 4 个方面包括从安全事件处理的开始一直到结束，于是“反黑客”一词应运而生。当我们掌握了新的工具并明白了如何使用新工具来攻陷网络，黑客的神秘面纱也将被揭开。

本书中每章都有一个连续的主题。每章的开篇是对讨论过的工具的总结，然后介绍新的工具。每章还对使用的技术进行了深入挖掘，为读者提供了最佳使用工具的信息，并且包括了在特定领域中使用工具时的忠告。案例研究用来演示在真实世界中如何恰当地使用工具。针对某些主题，笔者将为每种工具提供特定的案例分析。为了使案例研究尽可能真实，我们使用了文学性的描述，从而使得案例故事既具生动性又能够囊括足够多的工具。本书还提供了一些实例来讨论系统管理员在发生网络事故时的响应措施，读者可能会对这些措施产生质疑——这是不是最好的应急措施呢？因此，笔者需要提醒读者的是，我们无意提供针对安全事故或事件的反应措施的方法学或推荐意见，仅提供一个个有趣的案例研究以供阅读，从而有助于加强对某款工具使用的理解。

本书已经是第 3 版，对老读者而言，通过阅读本书，可以获得一些新的工具和介绍，当然对于新读者同样有益。第 3 版的改动包括：

- 为了更好的流程和组织，修改了章节布局
- 更新了本书中所有工具的内容
- 针对诸如 Netcat、tcpdump、Ethereal、nmap 和 hping 等工具加入了新的案例研究和示例
- 增加了新的工具，例如 THC-Amap、THC-Hydra、Trinux、Kismet、Ettercap、Wellenreiter、WinHex 和 X-Ways Trace 等
- 完全新增了针对防火墙的一章，包括防火墙概念的讨论、ipchains、iptables、IPFW 和 Cisco PIX 等

需要再次强调的是本书侧重于工具的使用而不是保证网络安全的方法学。因此，本书是由 Kevin Mandia、Matt Pepe 和 Chris Prosise 所著的 Hacking Exposed 系列和 Incident Response and Computer Forensics 的一本很好的丛书，因为那些书提供了本书所介绍工具的方法学基础。建议读者在试图理解这些工具之前，先阅读在那些书中讨论的方法学。但是，如果已经对这些方法学有一个大概的了解，在阅读本书时就没有障碍了。

另外，为了使用这些工具，我们需要讨论目前市场上最流行的操作系统是什么，以及在保护安全和调查取证现有网络时必须面临的其他操作系统。本书中，当提及 Windows 时，除非另有说明，都表示由 Microsoft 公司发布的所有操作系统，例如 95/98/Me/NT/2000/2003 和 XP。另一方面，当提及 Unix 时，表示任何类 Unix 的操作系统，而不仅仅是来自 Bell 实验室的原始版本。这些工具在某些 Unix 风格的系统上是有效的，包括 Solaris (i386 and Sparc versions)、Linux、FreeBSD、NetBSD、OpenBSD 和 Mac OS X 等。如果某款工具只能在 Unix 的某个版本上运行，我们会特意注明。

由于本书中介绍的工具在不久的将来可能都会有较大的变化(特别是那些开源的或者黑客工具)，所以本书提供了大量的截屏和输出。我们这样做并不是为了提供完全的材料，而是帮助读者在使用本书中讨论到的信息时匹配该工具的最新版本。

本书还提供了一个工具包(可访问 www.tupwk.com.cn/downpage/下载这个工具包)，它包括了书中提及的许多工具，这些工具的开发商或作者已经授权本书发布。如果讨论的工具需要商业授权，则提供的是一个开发商允许的试用版本。如果不能公开获得试用版本，则需要访问开发商的网站直接获取工具。由于开源运动蓬勃发展，我们在所提供的工具包和本书内容中尽量包含足够多的非商业工具，以便可以找到替代工具。我们希望所提供的工具包可以消除在获得这些工具以及定位对应网站时需要的大量争论。这会帮助指导你完成本书中列举出的任何示例。

如前所述，网络和安全工具持续更新，从而保持技术的发展。新的工具会出现，旧的工具会增加新功能。由于本书主要介绍网络和安全工具，我们希望有一种途径可以让读者了解到最新的工具、工具变化以及和安全相关的新闻。为了实现这个目标，我们提供了本书相应的网站www.antihackertoolkit.com。该网站提供了工具的链接、工具信息、本书错误更正和内容更新。

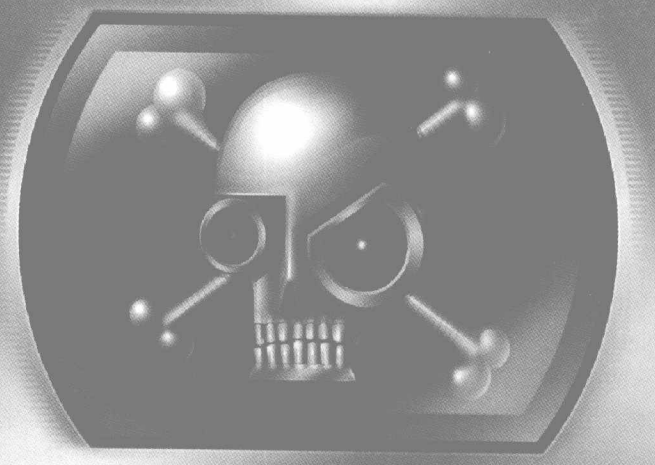
目　录

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。

1. 下载

Netcat 可以从多种途径获得，尽管许多 Unix 在发布时就已经安装了 Netcat 二进制代码，但最好的方法还是先获得 Netcat 的源代码，然后进行编译。因为在默认情况下，Netcat 源代码可能并未按照用户所需要的选项进行编译。因此，通过下载源代码并重新编译，就可以根据需要完全控制 Netcat 的功能。

可以从许多网站下载 Netcat，我们推荐一个可靠的网站：http:// www.vulnwatch.org/netcat/。

注意：

GNU Netcat 工程是原有的 Netcat 的重写版。其命令行选项与原来的 Netcat 相同，但只能在类 Unix 系统上编译，如 Linux、BSD 家族、Solaris 以及 MacOS X。它不能在 Windows 上编译。该版本可以在以下网站下载：http://netcat.sourceforge.net/。

2．安装

我们不详细讨论工具的下载、解包及安装，但是因为 Netcat 是我们所介绍的第一个工具，而且它具有一些需要关注的编译选项，所以有必要进行一些较为深入的讨论。

下载文件 nc110.tgz 后，创建一个文件夹并将其解包：

```
[root@originix tmp]# ls
nc110.tgz
[root@originix tmp]# mkdir nc
[root@originix tmp]# cd nc
[root@originix nc]# tar zxf ../nc110.tgz
[root@originix nc]#
```

注意：

与大多数 tar 包(使用 Unix 的 tar 工具创建的档案文件)不同，大多数 Netcat 并不创建自己的子目录，这一点看起来似乎并不重要，但如果所有的 tar 包(tarball)和子目录都已下载到同一个目录，就会发现 Netcat 把它所有的文件都放到了下载目录的根目录中，这样，清除这些文件将会是一件烦人的工作。

现在，开始准备编译。下面是两个重要的编译选项：

- **GAPING_SECURITY_HOLE**　当用作恶意目的时，该选项可使 Netcat 成为一个非常危险的工具，但同时也使 Netcat 的功能非常强大。激活这个选项后，Netcat 可以运行一个外部程序，而该程序的输入/输出(I/O)将会通过 Netcat 的数据管道流动，使得 Netcat 看起来像一个欺骗性的 inetd(端口监视程序)工具，只需要向相应的监听端口建立一个 TCP 或 UDP 连接，就可以执行远程命令(如启动一个 Shell)。这个选项默认情况下并不启用，因为一旦启用，就很可能滥用或配置错误。但如果正确使用，这个选项是相当重要的一个特性。
- **TELNET**　通常，如果使用 Netcat 连接到一个 Telnet 服务器(使用 nc *servername* 23 命令)，并不需要做太多的工作。在登录提示符出现之前，Telnet 服务器和客户端将会自动协商服务选项。通过激活这个选项，Netcat 可以对这些 Telnet 选项进行响应(通过对每个 Telnet 选项都回答 no 进行响应)，并且使得 Telnet 出现登录提示符。如果没有这个特性，那么当想使用 Netcat 和 Telnet 做一些有用的工作时，就必须使用脚本来响应这些 Telnet 选项。

到目前为止，这些选项可能对读者还没有什么明显的用处，但在了解了本章末尾的一些示例之后，您就会明白为什么我们要把这些选项提出来进行讨论了。

要激活这些选项，需要在 makefile 的开头加一行 DFLAGS 行。

```
# makefile for netcat, based off same ol' "generic makefile".
# Usually do "make systype" -- if your systype isn't defined, try "generic"
# or something else that most closely matches, see where it goes wrong, fix
```