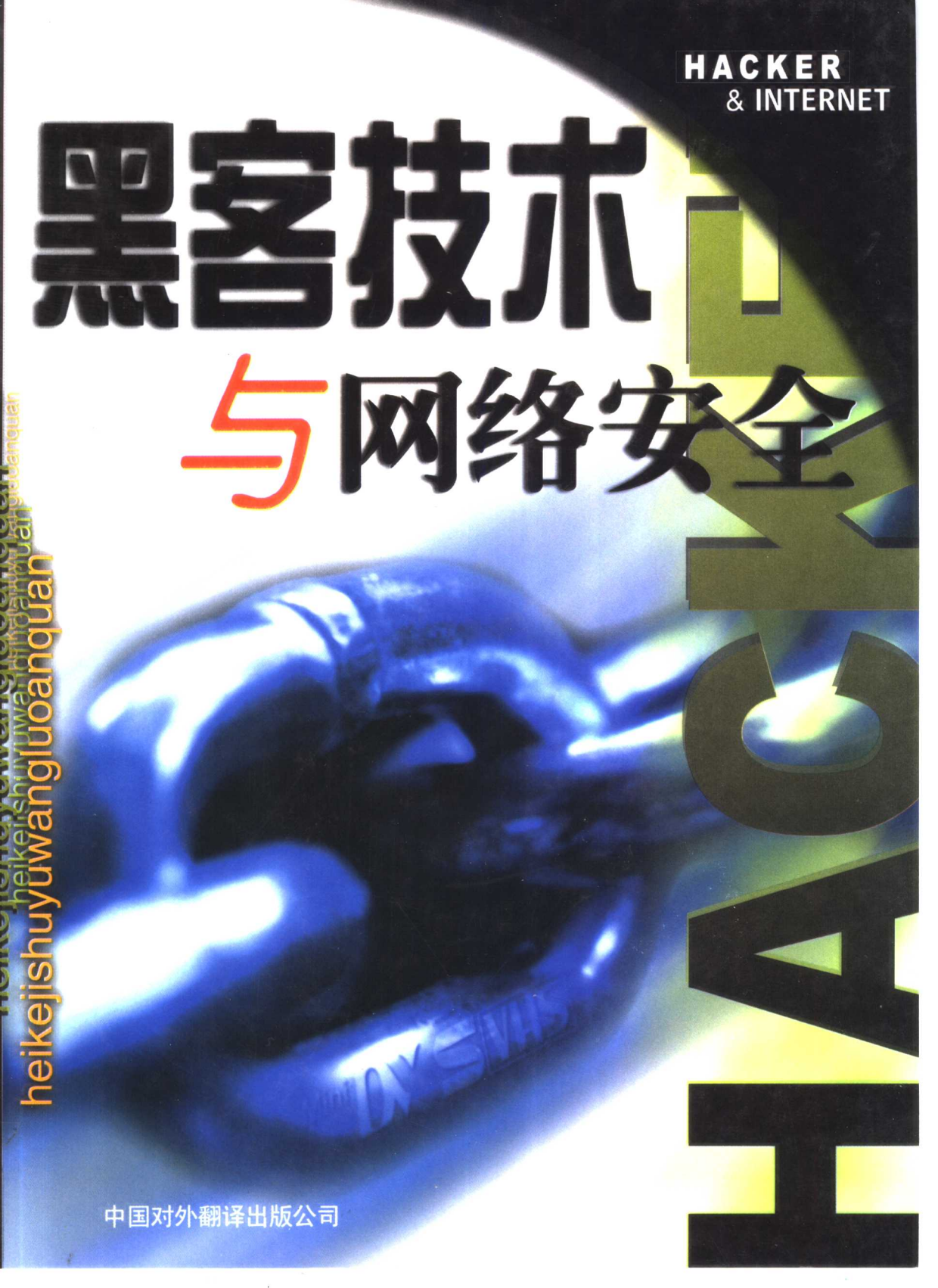
MWBOOK

HACKER
& INTERNET

黑客技术与网络安全



heikejishuyuwangluoanquan

heikejishuyuwangluoanquan

heikejishuyuwangluoanquan

HACK

MWBOOK.COM

08

中国对外翻译出版公司

黑客技术与网络安全

黑客技术与网络安全

杨守君 编 著

中国对外翻译出版公司

图书在版编目(CIP)数据

黑客技术与网络安全/杨守君编著.-北京:中国对外翻译出版公司,2000.4
ISBN 7-5001-0740-4

Ⅰ.黑… Ⅱ.杨… 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(2000)第 06355 号

出版发行/中国对外翻译出版公司
地　　址/北京市西城区太平桥大街 4 号
电　　话/66168195
邮　　编/100810
责任编辑/苏　醒
责任校对/姚成龙
封面设计/老　乡
印　　刷/北方工业大学印刷厂
经　　销/全国新华书店
规　　格/787×1092 毫米　1/16
印　　张/25.875
版　　次/2000 年 4 月第一版
印　　次/2000 年 4 月第一次印刷
字　　数/530 千字

ISBN7－5001－0740－4/G・195　定价:29.80 元

前　言

在全球信息技术高速发展的今天，黑客技术越来越受到关注。但是，由于历史的原因，人们对于黑客的认识存在着颇多的误解。本书试图通过正本清源，力图让更多的读者和计算机用户准确理解黑客及黑客技术，并对各种网络安全技术（黑客技术）进行介绍，分析原理，提供基本的实现方法；同时阐述了一些必要的防范技能。本书将使我们有一个较正确的认识，那就是：学会用黑客的头脑思考，掌握过硬的黑客技术，是提高网络安全、减少攻击带来的损失的最佳选择。

本书第一章对黑客与黑客文化进行了较深入的描述，对于初学者提供了正确导向，特别是更正了传媒上一些错误的观念。

接下来的三章提供了一些操作系统、编程方法、网络协议和网络编程等基本概念，旨在为以后各章的学习打下良好的基础。在操作系统一章中除了介绍 UNIX 的基本操作外，还介绍了 Linux 上的编程。因为 Linux 操作系统对网络通信做了很好的支持，并附带 gcc 编译器和 gdb 调试器，是最佳的选择。在 Linux 上编写的程序可以很短小，代码执行效率也很高。第三章介绍了 TCP/IP 协议，对 IP 和 TCP 的数据包格式作了简单的介绍。许多威胁网络安全的技术都是对协议的弱点攻击的。第四章介绍了网络编程。因为，在测试一个网络是否安全的同时，通常需要编个程序来完成一个特殊的测试工作。

接下来的 IP 地址欺骗也是根据协议的弱点进行的。

Sniffer 一章介绍了 Sniffer 的工作原理，通过利用 Sniffer 能收集到许多有用的信息。端口扫描一章除了介绍一些常用的网络命令之外，还介绍了端口扫描的几种技术。通过端口扫描同样能收集到相当丰富和有用的信息。口令一章讲解了口令破解器的工作原理。口令破解器是侵入一个系统比较常用的方法。特洛伊木马是侵入系统后留下的后门，为以后能再进入目标系统做准备。随后，介绍了缓冲区溢出攻击方法。这是一种很常用，也是很重要的攻击方法。本书对它们的原理作了比较详细的讲解。

再下来对攻击步骤作了一个总结，并讲述如何入侵 Windows NT。对前面章节中的方法的综合利用作了一些介绍，并提供了多个实例。之后介绍了计算机病毒的原理和防范。

SATAN 与 Internet 一章对 SATAN 这个 UNIX 程序进行全面的阐述，本章具有相对完整性，相信对每个 UNIX 平台的使用者都会有所帮助。

PGP 程序与个人信息加密一章对系统管理员来说非常重要。本章主要讲述 PGP 提供的各种不同的安全性方法，并讨论 PGP 密钥、PGP 安全性和已经知道的对 PGP 的攻击。

最后，在防火墙技术一章中，通过有关的介绍，使读者对该技术有一个全面的了解与掌握，以达到网络安全防护的目的。

本书相当一部分内容来自 Internet，经作者必要的加工整理，期望大家能正确看待黑客技术，同时，更好地承担维护网络安全的义务。

目　录

第一章　黑客与黑客文化

本章要点：

- 关于黑客的常规性问题
- 黑客文化介绍
- 黑客与网络安全

第一节　关于黑客(Hacker)

一、什么是黑客(Hacker)?

1. 怎么样才算是一位 Hacker?

在各种媒体上有许多关于 Hacker 这个名词的定义，它一般是指电脑技术上的行家或热衷于解决问题、克服限制的人。然而，如果你想知道如何成为一位 Hacker，有两件事是需要了解的。

这可以追溯到几十年前第一台微型计算机刚刚诞生的时代。那时有一个由程序设计专家和网络名人所组成的具有分享特质的文化族群。这一文化族群的成员创造了 Hacker 这个名词。他们建立了 Internet，创造出我们现在使用的 UNIX 操作系统，他们也使 Usenet 运作起来，并且让 World Wide Web 动起来。如果你是这个文化族群的一部分，如果你对这个族群有所贡献，而且这个文化的其他成员也认识你，并称你为 Hacker，那么你就是一位 Hacker。在精神上，Hacker 并不单指(或限制于)这种软件 Hacker 的文化。有人也把 Hacker 的特质发挥在其他领域，例如，在电子或者音乐方面。事实上你会发现，在任何一种科学或艺术的最高境界，你都可以发现 Hacker 的特质。软件 Hacker 们认为，那些类似的精神也都可以称为“Hacker”。有些人还主张 Hacker 的通性是独立于任何媒介之上的，不特别属于任何一种 Hacker 所在的环境。

在另一个团体，他们的成员也很大声地称自己为 Hacker，但是他们并不是真的 Hacker。

这些人(大部分是男性青年)专门闯入电脑或入侵电话系统，真正的 Hacker 们称他们为入侵者 (Cracker)，并且不愿意和他们在一起做任何事。Hacker 们认为这些人懒惰、不负责任，

并且不够光明正大;他们认为,能破解安全系统并不能使你成为一位 Hacker。但是不幸的是,很多记者和作家不明究理地使用 Hacker 这个词来描述 Cracker 们,这让真的 Hacker 们很愤怒。

基本上,Hacker 和 Cracker 之间最主要的不同是:Hacker 们创造新东西,Cracker 们破坏东西。

如果你想要成为一位 Hacker,继续读下去吧。如果你想要成为一位 Cracker,那么就去读 alt.2600 newsgroup(国外著名破坏团体 2600 的新闻组),并准备在你发现自己并不如想像中那么出色时,给自己一点客观评价。所有关于 Cracker 的事情就只有这些了。

2.Hacker 态度

Hacker 们解决了问题并创造新东西,他们相信自由并自愿互相帮助。想要被别人接受成为一位 Hacker,你必须发自内心地表现出这种态度。为了很自发地表现出这种态度,你必须先完全认同这些态度。

如果你只是把学习 Hacker 态度这件事当作一种能在这个文化中赢得认同的途径,那么你已经忽略了真正的重点。由衷地接受这些态度是很重要的,这能帮助你学习并维持你的动机。就像那些具有创造性的艺术一样,成为一位大师的最有效方法是学习大师们的精神。

所以,如果你想要成为一位 Hacker,请反复地做下面的事情,直到你完全领会它们为止:

(1)这世上充满着很多未被解决的问题。

作为一个 Hacker 是充满快乐的,但这是一种因为努力得到成果所带来的快乐。努力的成果则带来动机。成功的运动家的动机来自于使他们的身体不断进化,并把自己推向物理上的极限所带来的快乐。与此相同,要想成为 Hacker,你必须能从解决问题、精进技术和运用知识的过程中感受到一种悸动。

如果你不是天生就能感受到这种悸动的人,那么,为了要成为 Hacker,你必须使自己变成这样的人。否则,你会发现你的 Hacker 精神就会像性、金钱、社交活动一样,因为分心而被消磨掉。

你也必须为你的学习能力建立一种信念,直到完成你的工作——即使你只处理一小部分,并且你也不知道到底还要学些什么东西才有办法解决你的问题,但是你会努力学习,准备充足,以应付下一个问题。

(2)没有任何人必须一再地解决同一个问题。

富于创造力的头脑是贵重而有限的资源。世界上有这么多的新问题在等着被解决,因此富于创造力的头脑不该被浪费地用来重复发明轮子。

身为一位 Hacker,你必须了解到其他 Hacker 们的时间也是很宝贵的——所以,分享资讯,解决问题和提供解决方案给其他 Hacker 以解决新的问题,这些几乎算是道义上的责任。

即使 Hacker 们所拥有的大多是从其他 Hacker 的身上得来的,也并不意味着你必须把你创造的作品全部交出来。你可以卖出足够数量的产品,以求得温饱,给付房租和买电脑设备,

这和 Hacker 的价值观并不相违背。使用你的 Hacker 技能以维持一个家庭的生活，甚至致富，只要你仍不忘记你是一位 Hacker，那么这些行为并不会产生矛盾。

(3)无聊而单调的工作是有害的

Hacker 们(有创造力的人也是一样)永远不该做一些无聊而单调并且愚蠢的重复性工作。如果这样的事情发生的话，这表示他们正在做一些不该做的事，Hacker 应该解决新的问题。

要成为一位 Hacker，就要尽可能地自动避免无聊，对此你必须有相当的认知。这不只是为了你自己，也是为了所有的人(尤其是其他的 Hacker)。

有时候也会有例外。有时候，Hacker 们会去做一些被认为无聊或重复性的工作，当作脑力的训练，或是为了要学习某种技能或某种特殊经验。不过这是一种选择，任何人都不该被强迫面对无聊的事。

(4)自由很重要

Hacker 们天性上是反对独裁的。任何一个给你下命令的人就都给你一个独裁式的工作，并且可以给你一些愚蠢的理由，阻止你解决任何吸引你的问题。所以任何独裁式的行为都会受到批判，以免会危害到你和其他的 Hacker 们。这和为反对而反对是不同的。小孩子需要被指导和阻止他们犯错；Hacker 也会同意接受某种权威，照着指示做，以较短的时间得到自己想要的，不过那是一种有限且理性的协定。

专制在监察和保密这种问题上是很有效的方法。这些行使专制的人并不相信自愿性质的合作和资讯分享——他们只相信在他们控制之下的合作关系。所以，身为一位 Hacker，你必须具有一种敌对的天性，以对抗监察、秘密和使用外力强迫或迷惑你的人的行为；你必须以互信作为你行为的基础。

(5)态度并非不等效于能力

要想成为一位 Hacker，你必须开始培养这些态度。但是，如果你只是单独地模仿某一种态度，这并不能使你成为一位真正的 Hacker，也不会使你成为一位运动冠军或摇滚明星。

因此，你必须学会猜疑态度和尊敬各种能力。Hacker 们不会浪费时间在虚华的人身上，他们尊敬的是能力——特别是身为 Hacker 的能力；但对于其他方面的能力也充满敬意。如果有能力追求一些很少有人能弄懂的技术，追求精神上的技巧，并能集中精力，那就再好不过了。

如果你尊敬各种能力，那么你就会乐于自己发展这些能力——这会使你的努力和奉献成为一种刺激性的消遣，而非一份苦差事。这对于想要成为 Hacker 的人而言是很重要的。

二、黑客守则

(1)不恶意破坏任何系统。这样做只会给你带来麻烦。恶意破坏他人的软件将导致法律追究。注意：千万不要破坏别人的文件或数据。

(2)不修改任何系统文件。如果你是为了要进入系统而修改它，请在达到目的后将它复原。