电脑报 总策划

黑客攻防大师

第二版

彻底了解黑客手法并进行有效的防范

熊菲 编著

由资深黑客撰写的闯关宝典，带你过关斩将，势如破竹
黑客世界云谲波诡，尔虞我诈，让你练就火眼金睛洞悉人心
真枪实弹，身临其境，虚拟环境搭建合法的黑客训练营
所有演示经过多次严格测试，绝不告诉你无法做到的方法

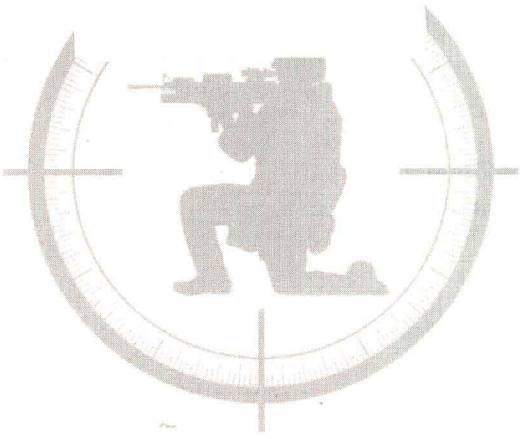
黑客之道 从入门到精通

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

黑客攻防大师

第二版

彻底了解黑客手法并进行有效的防范



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

黑客的出现可以说是当今信息社会中有目共睹、不容忽视的独特现象。一些黑客的网络袭击行为有意或无意地对社会造成了不同程度的危害。为了捍卫信息社会的安全，本手册以客观实例为基础，结合了作者长期实践的心得体会，从多个角度来分析了黑客“攻”与“防”的全过程，包括：扫描、系统漏洞、远程控制、木马连接、木马防杀、痕迹清理、嗅探捕获、网站入侵、加密解密等内容。

本手册绝不是为那些动机不良的人提供支持，而是最大限度地唤醒人们的网络安全意识，以让广大网民共同重视信息安全存在的威胁，并有效防范。

警告：使用网络技术攻击他人计算机属于违法行为，切勿用本手册介绍的相关操作对他人计算机进行恶意攻击，否则后果自负！

光盘要目

1.扫描与字典工具　　2.远程控制工具
3.加花工具　　4.伪装工具
5.代理与虚拟机　　6.嗅探工具集合
7.加密与解密工具

黑客攻防大师(第二版)

编　　著：熊　菲
技术编辑：何　磊
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：苏州新海博数码科技有限公司
文本印刷：重庆联谊印务有限公司
开本规格：787mm×1092mm 1/16　22印张　400千字
版　　号：ISBN 978-7-89476-175-0
版　　次：2009年7月第1版　2009年7月第1次印刷
定　　价：35.00元(1CD+手册)

前言

如今“黑客”一词已经让许多网民闻之色变了，因为指不定哪时你的游戏账户会不翼而飞，隐私信息被人偷偷曝光，邮件也被人恶意截取……层出不穷的黑客事件已经让人们开始重视黑客带来的威胁。为了不让自己成为任人宰割的“肉鸡”，为了追回失去的信息财富，为了维护尊严给入侵者正义的反击，通晓黑客技术也成为网上谋生的一种手段。

很多读者都会有一个疑惑：尽管翻阅了很多黑客技术书籍，但仍然觉得徘徊在黑客世界外。这是可以理解的，其实大家都明白只有当理论与实践相结合才能融会贯通，可是要靠入侵他人计算机来践行所学到的知识却是违法行为，因此很多读者并没有实践的机会。此外，黑客技术关联较广，涉及到计算机技术的方方面面，可谓是博大精深，例如在介绍木马入侵的时候，就会谈到不同网络环境中木马连接的方法，其中牵涉到如网关、端口映射、动态域名等一系列网络概念，等讲到木马防杀的时候又要先了解特征码、加壳、加花等汇编知识。可想而知，对于初学者来说，当然会感到云里雾里不知如何学起，这就是为什么不少读者感到黑客入门难的原因了。

为了让读者了解和熟悉黑客攻击手段，我们出版了《黑客攻防大师》第一版，该版非常注重知识的系统性，开篇即为读者排解网络基础中的诸多疑难，接着再教大家模拟真实的网络环境以备实践，然后全面介绍黑客的攻防实战，这样的编排使得整体上层次分明，既让读者能亲手实践所学知识，也让读者不再为某个专业术语而中途“卡壳”。另外，在章节上也将黑客的主要行为进行拆分，大致包括捕捉目标、尝试连接、完全控制、留下后门以及清理足迹等一系列过程，以让读者对黑客入侵的思路有个清晰的轮廓。值

得一提的是，在编写的时候，我们主要向读者介绍黑客技术中所涉及的思考方法，而非简单机械地告诉读者某个黑客工具该怎么用，某个漏洞黑客是如何入侵的。要知道工具是死的，漏洞是可以修补的，环境也是可变的，只有掌握了黑客入侵的思路，才能防范并追踪黑客。

《黑客攻防大师》第一版自面市以来深受广大读者肯定与好评。不过第一版也未尽完美，在这次重新编写的《黑客攻防大师》第二版里，我们对内容结构进行了优化，删除第一版中的冗余篇章，并增添了许多实用性内容。针对读者的反映情况，重点介绍了大多数人感兴趣的几个黑客热点问题：组建虚拟局域网、Windows XP 的认证入侵、缓冲区溢出获取权限、木马连接、木马防杀、嗅探数据以及网站入侵。可以说第二版是第一版的升级，除了体现从入门到精通的理念外，其主题更加突出，内容的广度与深度均得到了改善。

在黑客攻防战中，从来都是“道高一尺魔高一丈”，随着版本的更新，技术的变革，在介绍的案例中没有哪个是永远成立的，唯一不变的是基本原理和黑客思想，在介绍黑客攻防的时候，作者也尽量剖析黑客的想法与行为，以帮助读者思考，如此才能对症下药，治标亦治本。

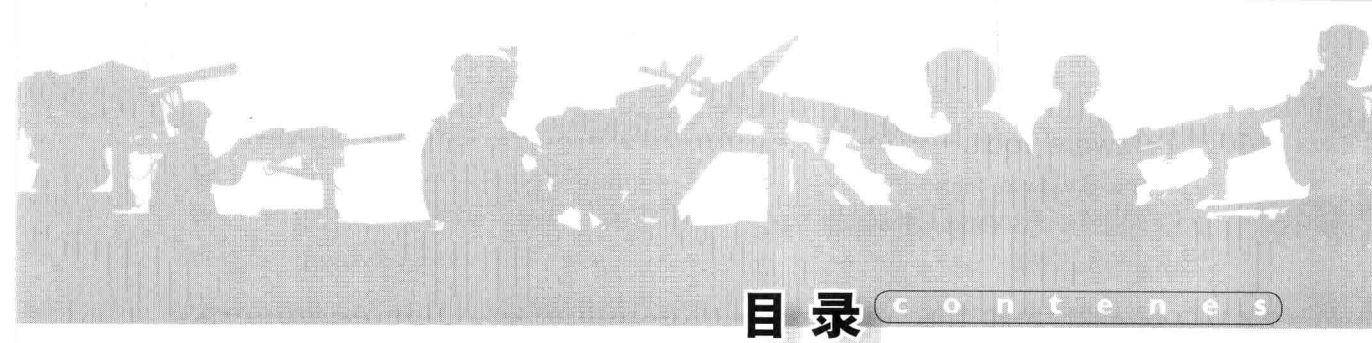
有江湖的地方就有是非，维护网络安全是一件任重道远的事情，我们希望读者能够最大限度地提高网络安全意识，共同维护网络安全！

在这里，我们再次提醒各位，切勿将我们探讨的黑客技术用于任何非法目的，否则必须承担各种相关的法律责任，切记切记！

编者

2009.6

此为试读，需要完整PDF请访问：www.ertongbook.com



目录 contenes

第1章 黑客入门基础

第2章 打造黑客训练营

第3章 信息扫描与目标锁定

第4章 认证与系统漏洞的入侵

第5章 远程控制目标系统

第6章 木马开启后门的入侵

第7章 木马的伪装与防杀

第8章 行踪隐藏与痕迹清理

第9章 嗅探器截取数据信息

此为试读，需要完整PDF请访问：www.ertongbook.com

第10章 QQ攻防实战

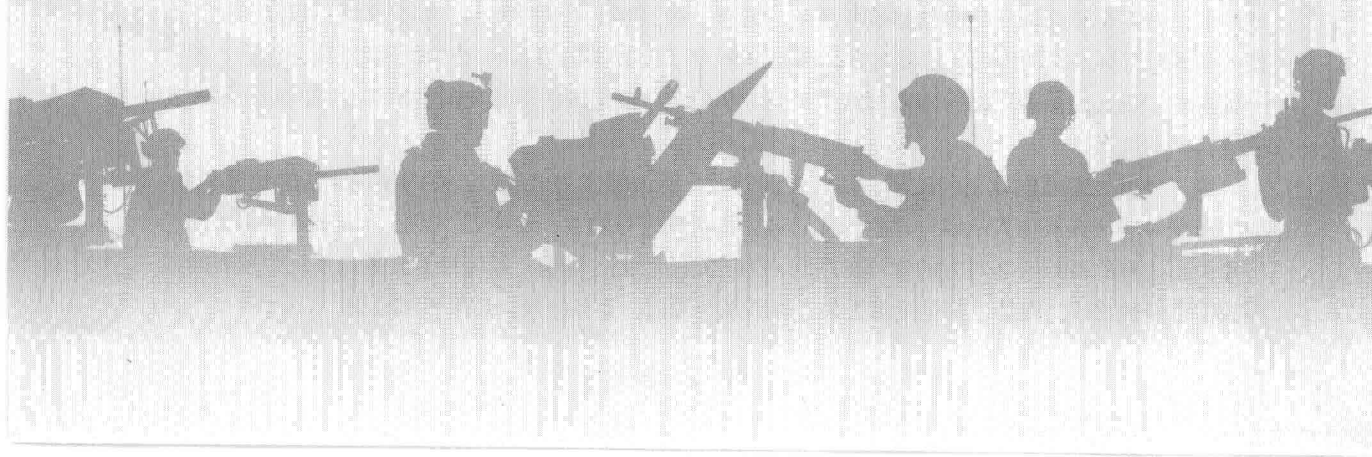
第11章 电子邮件破解与欺骗

第12章 网站入侵技术分析

第13章 密码破解与防范

第1章
黑客入门基础

互联网的发展让人们的学习、工作和生活发生了巨大变化，不过网络安全问题也随之凸现而来，总有不法分子威胁着人们的信息安全。他们是如何在网络中兴风作浪的呢？我们将在本章做初步介绍。



1.1 网络中的黑客

Internet（因特网）的普及使人们的工作生活发生了翻天覆地的变化，可是在 Internet 世界中却没有人来管理。如同武侠小说中的“江湖”一样，在这个没有王法的世界中滋生出了许多正派和邪派的力量，他们有秩序的建立者，也有潜在的破坏者，他们被人们统称为——黑客。下面让我们走进黑客的世界，一同揭开黑客神秘的面纱。

1.1.1 什么是黑客

在人们眼中，黑客是一群专业技能超群、聪明绝顶、精力旺盛的年轻人，致力于破译各种密码，查找各种系统漏洞，以便偷偷地、未经允许地闯入政府、企业或他人的计算机系统窥视他人的秘密数据。那么什么是黑客呢?

黑客，英文名为 Hacker，是指对计算机信息系统进行非授权访问的人员。人们通常认为黑客是指在计算机技术上有一定特长，并凭借自己掌握的技术知识，采用非法的手段逃过计算机网络系统的存取控制，而获得进入计算机网络进行未授权的或非法的访问的人。

早期的黑客主要入侵程控电话系统，找出其中的漏洞，借以享受免费的电话业务。随着计算机网络的诞生和发展，他们对网络产生了越来越浓厚的兴趣。最初他们闯入他人计算机系统的本意不在攻击对方和造成破坏，而是凭借自己的专业技能发现其中的漏洞，进入系统后留下一定的标记，以此来炫耀自己的能力。

20 世纪 60 年代，在美国麻省理工学院的人工智能实验室里，有一群自称为黑客的学生们以编制复杂的程序为乐趣，当初他们并没有功利性目的。此后不久，连接多所大学计算机实验室的美国国防部实验性网络 APARNET 建成，黑客文化便通过网络传播到更多的大学乃至社会。后来，有些人利用手中掌握的“绝技”，借鉴盗打免费电话的手法，擅自闯入他人的计算机系统，干起见不得人的勾当。随着 APARNET 逐步发展成为因特网，黑客们的活动天地越来越广阔，人数也越来越多，形成鱼龙混杂的局面。近年来，随着因特网在全球的飞速发展，各种恶性的非法闯入事件更是频频发生，对世界各国计算机系统的安全构成极大的威胁，于是在人们的心目中，黑客的形象也就被抹了黑。

黑客侵入计算机系统是否造成破坏以及破坏的程序，因其主观动机不同而有很大的差别。的确有一些黑客纯粹出于好奇心和自我表现欲而闯入他人的计算机系统，他们可能只是窥探一下别人的秘密或隐私，并不打算窃取任何数据和破坏系统。另有一些黑客出于某种原因，如泄私愤、报复、抗议而侵入和篡改目标网站的内容，羞辱对方。例如 1999 年 5 月以美国为首的北约炸毁我驻南使馆后，曾有一批自称“正义的黑客”纷纷闯入白宫、美国驻华使馆、美国国防部和美国空军等官方网站，篡改其主页，以示抗议。

第三类就是恶意的攻击和破坏，其危害性最大，所占的比例也最大。有的谋取非法的经济利益，如盗用账号非法提取他人的银行存款，或对被攻击对象进行勒索，使个人、团体、国家遭受重大的经济损失，还有的蓄意毁坏对方的计算机系统，为一定的政治、军事、经济目的服务。系统中重要的程序数据可能被篡改、毁坏，甚至全部丢失，导致系统崩溃、业务瘫痪，后果不堪设想。

图1-1 在互联网上黑客总是让人害怕

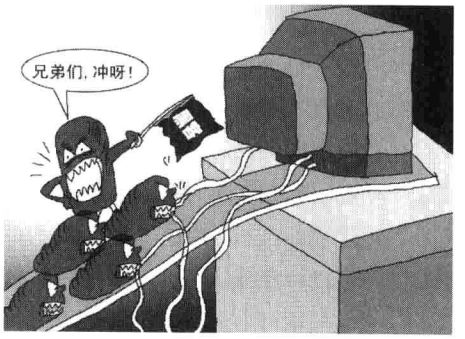


图1-2 病毒也是黑客入侵的利器

1.1.2 黑客攻击的过程

黑客在面对不同环境时所采取的攻击手段也会不同，但纵观其整个攻击过程，也有一定的规律可循，一般可以分：攻击前奏、实施攻击、巩固控制、继续深入几个过程。下面具体了解一下这几个过程。

1.攻击前的准备

黑客在发动攻击前了解目标的网络结构，搜集各种目标系统的信息等。

（1）锁定目标：网络上有许多主机，黑客首先要寻找他站点。当然能真正标识主机的是 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。

（2）了解目标的网络结构：确定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关路由，哪里有防火墙、入侵检测系统（IDS），哪些主机与要攻击的目标主机关系密切等，最简单的就是用 Tracert 命令追踪路由，也可以发一些数据包看其是否能通过来猜测防火墙过滤规则的设定等。当然老练的黑客在干这些的时候都会利用别的计算机来间接地探测，从而隐藏他们真实的 IP 地址。

（3）搜集系统信息：在搜集到目标的第一批网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。搜集系统信息的方法有开放端口分析，利用信息服务，利用安全扫描器，社会工程。

接着黑客还会检查其开放端口进行服务分析，看是否有能被利用的服务。因特网上的主机大部分都提供 WWW、E-mail、FTP、Telnet 等日常网络服务，通常情况下 Telnet 服务的端口是 23 等，WWW 服务的端口是 80，FTP 服务的端口是 21。

（4）利用信息服务：像 SNMP 服务、Traceroute 程序、WHOIS 服务可用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节，Traceroute 程序能够用该程序获得到达目标主机所要经过的网络数和路由器数，WHOIS 协议服务能提供所有有关的 DNS 域和相关的管理参数，Finger 协议可以用 Finger 服务来获取一个指定主机上的所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等）。所以如果没有特殊的需要，管理员应该关闭这些服务。

利用安全扫描器，搜集系统信息当然少不了安全扫描器。黑客会利用一些安全扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞、应用软件漏洞、CGI、弱口令用户等。

2.实施攻击

当黑客探测到了足够的系统信息，对系统的安全弱点有了解后就会发动攻击，当然他们会根据不同的网络结构、不同的系统情况而采用不同的攻击手段。一般黑客攻击的终极目的是能够控制目标系统，窃取其中的机密文件等，但并不是每次攻击黑客都能够达到控制目标主机的目的的，所以有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作。关于黑客具体采用的一些攻击方法，我们将在各章中进行介绍。

3.巩固控制

黑客利用种种手段进入目标主机系统并获得控制权之后，不是像大家想象的那样会马上进行破坏活动，删除数据，篡改网页等，那是毛头小伙子们干的事情。一般入侵成功后，黑客为了能长时间地保留和巩固他对系统的控制权，而且不被管理员发现，他会做两件事：清除记录和留下后门。日志往往会记录一些黑客攻击的蛛丝马迹，黑客当然不会留下这些“犯罪证据”，他会把它删了或用假日志覆盖它，为了日后可以不被觉察地再次进入系统，黑客会更改某些系统设置，在系统中植入特洛伊木马或其他一些远程操纵程序。

4.继续深入

用清除日志，删除复制的文件等手段来隐藏自己的踪迹之后，攻击者就开始下一步的行动——窃取主机上的各种敏感信息，如软件资料、客户名单、财务报表、信用卡号等，也可能是什么都不动，只是把你的系统作为他存放黑客程序或资料的仓库，也可能黑客会利用这台已经攻陷的主机去继续他下一步的攻击，如继续入侵内部网络，或者利用这台主机发动 D.O.S 攻击使网络瘫痪。

网络世界瞬息万变，黑客们各有不同，他们的攻击流程也不会完全相同，这 4 个攻击步骤是对一般情况而言的，是绝大部分黑客在正常情况下采用的攻击步骤。

1.2 认识IP地址

前面我们了解了什么是黑客，黑客进攻的步骤。不过黑客种种活动都基于网络平台，所以要真正了解黑客攻击手段，必先学习网络基础知识。IP 协议是最重要的网络协议，下面我们就从 IP 协议学起。

1.2.1 什么是IP地址

在现实生活中，人们会以名字的方式来区分不同的个人，实际上，同名同姓的人大有人在，为了在人口统计上绝对地区分，人们就使用了身份证，身份证上有唯一对应个人的号码，这样就完全区分了每个人。

同样，在 Internet 中，也有许多电脑使用同样的名字，为了严格区分它们，人们就为电脑使用了

此为试读，需要完整PDF请访问：www.ertongbook.com