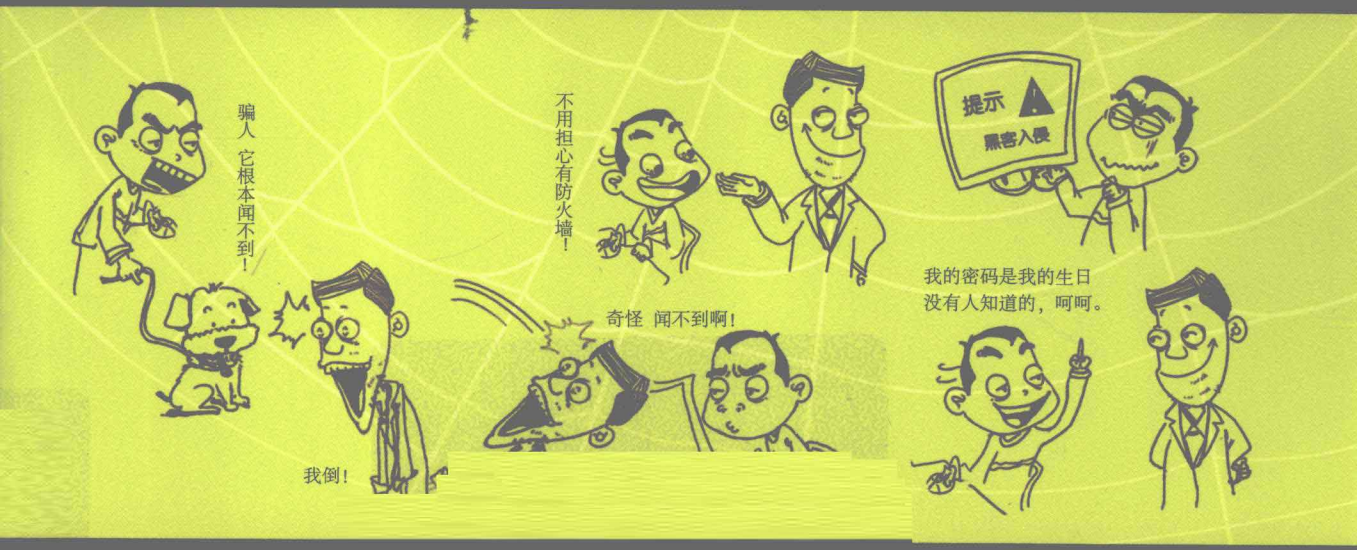
安全宝典 新手必备

本书是了解黑客，学习安全知识的一把金钥匙！

# 黑客工具全程揭秘

张齐 编著

扫描工具、QQ工具、嗅探工具、注入工具、杀毒工具、木马工具……一应俱全




- 结合丰富案例， 上手更加简单
- 穿插生动漫画， 降低学习难度
- 一本书籍在手， 黑客工具全懂

此书秉承黑客理念，贯穿黑客入侵全过程，意在让广大读者了解黑客是如何入侵、攻击的，并给出相应的防护方法。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

张齐 编著

# 黑客工具全程揭秘

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 简 介

本书分10章围绕当前黑客主流工具展开，囊括最新的攻击手段和防护技巧，涵盖了从系统底层到网络应用层的多方面知识。

本书主要针对掌握基础计算机知识，对网络安全兴趣浓厚的朋友；对黑客技术感兴趣，但未经过系统学习的读者；网络攻击与防护初级学者以及网络管理者。

**图书在版编目（CIP）数据**

黑客工具全程揭秘 / 张齐编著. -- 北京：中国铁道出版社，2012.1

ISBN 978-7-113-12885-2

Ⅰ. ①黑… Ⅱ. ①张… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2011）第077412号

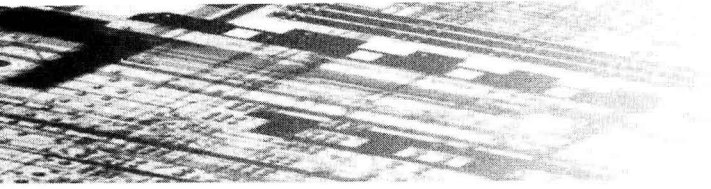
**书　　名：黑客工具全程揭秘**
**作　　者：张　齐　编著**

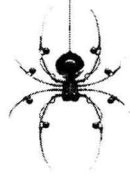
**责任编辑：苏　茜**　　**读者热线电话：010-63560056**
**编辑助理：尚世博**
**封面设计：张　丽**　　**责任印制：李　佳**

**出版发行：中国铁道出版社（北京市西城区右安门西街8号　　邮政编码：100054）**
**印　　刷：三河市华丰印刷厂**
**版　　次：2012年1月第1版　　2012年1月第1次印刷**
**开　　本：787mm×1092mm　1/16　　印张：16.75　字数：389千**
**书　　号：ISBN 978-7-113-12885-2**
**定　　价：38.00元**

**版权所有　侵权必究**

凡购买铁道版图书，如有印制质量问题，请与本社发行部联系调换。





# 前 言
## Foreword

黑客对于大多数人来说是个神秘的词汇。他们隐藏在网络中的角落，通过一根网线来掌控着他们希望掌控的对象。入侵、病毒、木马、嗅探、钓鱼……的网络威胁已经危及到每位网民。

你是否很想知道黑客的入侵是如何实现的？是否想知己知彼以便确保自己的网络更安全？编写此书将秉承黑客惯用的工具，贯穿黑客入侵思路，告诉广大用户黑客是如何入侵攻击的，并告诉大家防护的方法。

### 读者对象明确

- 掌握基础计算机知识，对网络安全兴趣浓厚的朋友。
- 对黑客技术感兴趣，但未经过系统学习的读者。
- 网络攻击与防护初级学者以及网络管理者。

### 内容涵盖范围广

本书根据目前黑客习惯的攻击方式分类，包括黑客文化介绍、安全基础知识、扫描工具、注入工具、嗅探工具、QQ 工具、木马工具、加密解密工具、远程控制工具以及安全工具等几大方面，全面剖析当前主流的攻击方式，并给出面对每种攻击的防护方法。

### 讲解紧贴实战

由于目前很多入侵者习惯于工具的使用，而对于用户来说掌握这些工具是提高防御能力的一个途径，所以我们将目前常见的黑客工具做了分类。

### 网络安全第一

全书旨在技术讨论，不涉及任何主观攻击，望请广大读者抱以技术学习的初衷阅读本书，黑客技术本身并不神秘，黑客工具只是其实现目的的一种手段，防御与攻击的关键在于人，而非软件。正确地运用它们，不但可以提高计算机水平，更可以了解一个全新的世界。

最后，我想用电影《蜘蛛侠》中男主角帕克的几句话作为结束语，以此送给所有网络安全爱好者以及那些一直致力于网络安全工作者们：

With great power comes great responsibility（能力越大责任越大）

Who am I？（我是谁？）

I'm Hacker！（我是黑客！）

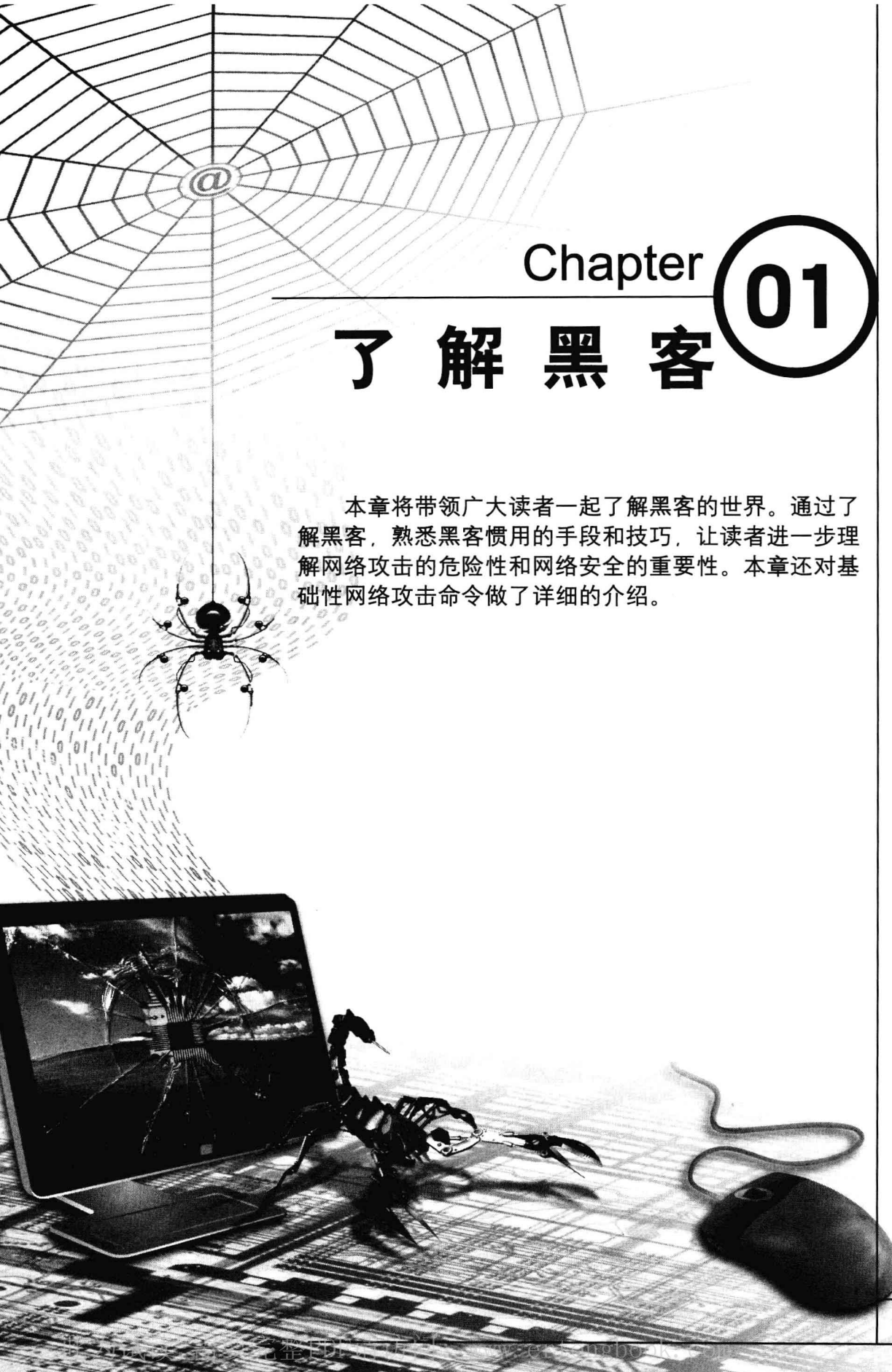
编 者

2011 年 11 月

# 目 录
Contents



此为试读，需要完整PDF请访问：www.ertongbook.com



Chapter 01

# 了解黑客

本章将带领广大读者一起了解黑客的世界。通过了解黑客，熟悉黑客惯用的手段和技巧，让读者进一步理解网络攻击的危险性和网络安全的重要性。本章还对基础性网络攻击命令做了详细的介绍。

## 1.1 黑客简介

也许你还不了解黑客，也许你还不曾被攻击过。但是在广阔的互联网中，每时每刻都发生着网络攻击。越来越多的网络威胁袭来，漏洞、病毒、木马、陷阱……令人防不胜防。这后面隐藏的攻击者，人们往往称之为“黑客”。了解黑客的行为和习惯，可以更好地了解黑客这个概念……

### 1.1.1 是黑客不是骇客

在浩瀚的互联网中，计算机安全越来越受到人们的关注，而黑客技术也随着网络的发展而日益强大起来。

目前很多黑客在进行网络攻击的过程中，都使用了专用工具，这样就降低了入门门槛。

首先了解一下什么是黑客。黑客这个概念最早源自英文 hacker，早期在美国的电脑界是带有褒义的。但在现在的媒体报导中，黑客一词往往指那些“软件骇客”(software hacker)。事实上，现在的“软件骇客”更多地被称做 cracker，该群体以破坏软件版权保护为目的，而且对软件加解密技术非常熟悉。

黑客一词，原指热心于计算机技术，水平高超的计算机专家，尤其是程序设计人员。黑客和骇客的根本区别是：黑客们修补漏洞，而骇客们利用漏洞进行破坏。

所以首先需要读者建立的观念就是，黑客并不是仅仅作为攻击者出现，更多的是为了保障网络安全出现的。


**真正的黑客绝对不是破坏者，而他们利用攻击工具也是为了获取更多的安全信息，推动网络安全的发展。**

有名的黑客很多，接下来就列举一些代表人物，帮助大家理解黑客的世界。

**1．凯文·米特尼克**（见图 1-1）

凯文·米特尼克，这位“著名人物”现年不过 45 岁。其实他的技术也许并不是黑客中最好的，而且相当多的黑客都反感他，认为他是只会用攻击、不懂技术的攻击狂，但是其黑客经历足以让全世界为之震惊，也使得许多网络安全人员丢尽面子。

在他 15 岁的时候，仅凭一台计算机和一部调制解调器就闯入了北美空中防务指挥部的计算机系统主机，接着又在很短的时间里，连续进入了美国 5 家大公司的网络，最后联邦调查局不得不联合其他黑客将其诱捕。因为政府认为：让凯文·米特尼克拥有自由的网络实在是太可怕了。

**2．林纳斯·托瓦兹**（见图 1-2）

说到林纳斯·托瓦兹就不得不提著名的 Linux 操作系统。与很多黑客不同，托瓦兹行事低调，但他的技术不能小觑，应该说林纳斯·托瓦兹更多的是一位电脑程序员。他对于技术的执着绝非一般人能企及。

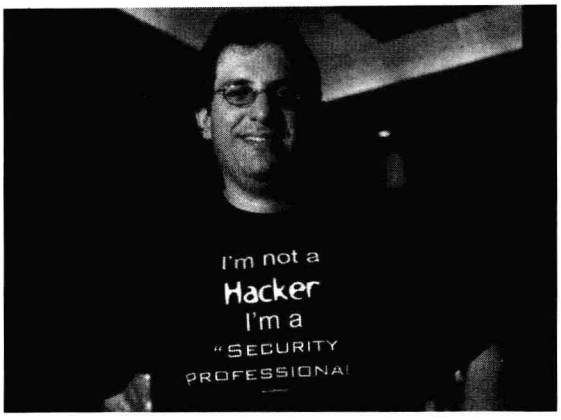



图 1-1 凯文·米特尼克

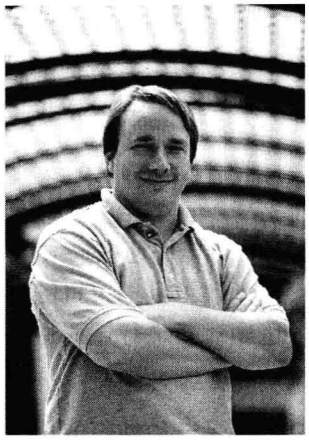


图 1-2 林纳斯·托瓦兹

3. 小榕

虽然小榕的影响力远没有前两位深远，但就国内来说，他绝对是位黑客技术专家。他的黑客原则是："不能仇视社会，不能给别人制造麻烦，不能给别人带来损失。"有人对黑客这样评价：黑客是一种不断研究不断探索的境界。

他的作品有乱刀、流光、溯雪、流影，这些工具都可谓大名鼎鼎。他曾经在一个月里进入1000 家网站，并找出其中的漏洞。小榕的名字在网上非常响亮，因为他发布了许多杀伤力巨大而又极易上手的黑客工具。

## 1.1.2 黑客宗旨：网络资源共享

黑客的宗旨就是网络资源的共享。比如入侵了网站后提醒站长修补漏洞，不搞破坏，攻防兼备。真正的黑客精神，是要让人类超越计算机，成为计算机的主宰，而不是成为计算机或者利益的奴隶。

## 1.1.3 黑客常用哪几招

黑客在进行网络攻击时手段繁多，花样不断，由此产生很多安全问题。不过归纳起来，攻击手段一般分为以下几类：

1. 口令入侵

这种入侵方式最为直接有效。就是通过使用合法账号的口令进入主机，然后再实施攻击活动。这种入侵方法的前提是必须要有正确的账号和口令，而获得口令的方法非常多，比如监听、木马控制等。

通过协议监听方式，虽然操作起来比较简单，但成功率并不高，攻击者往往采用中途拦截的方式获取账号和口令。因为很多协议根本就没有采用任何加密手段，如 Telnet、FTP 等在进行数据传输时就会造成被监听的危险。

还有一种方法是强行破解用户口令，这种采用穷举法的暴力破解方式相当流行，利用字典方式破解也是一种有效率的方法（见图 1-3）。

字典的这种穷举破解方法为用户数据安全带来了比较大的影响，不过如果我们将密码设置得足够复杂，完全有可能逃过这种暴力破解。

### 2．扫描漏洞

目前，大多数电脑安装的是 Windows 操作系统，其系统的稳定性和安全性随着版本的提升而提高，但安全隐患却一直存在，看看微软官方网站公布的补丁就可知一二。黑客通过专业的工具，可以快速扫描大量 IP 地址下电脑的漏洞，再进行病毒和木马的植入以达到入侵目的。

在了解了目标主机的漏洞和弱点之后，黑客就能使用缓冲区溢出和测试用户账号和密码等，达到对其进行试探性攻击的目的。

### 3．木马入侵

木马是一种能窃取用户本地信息的特殊程序，也是目前最为广泛的入侵途径。黑客通过木马程序可以轻易地入侵并控制用户计算机，并在用户不知情的状况下通过用户的计算机进行各种破坏活动，熟知的 QQ、网游账号被盗，基本上都是木马做的手脚，比如大名鼎鼎的灰鸽子软件，就是一款典型的木马程序（见图 1-4）。

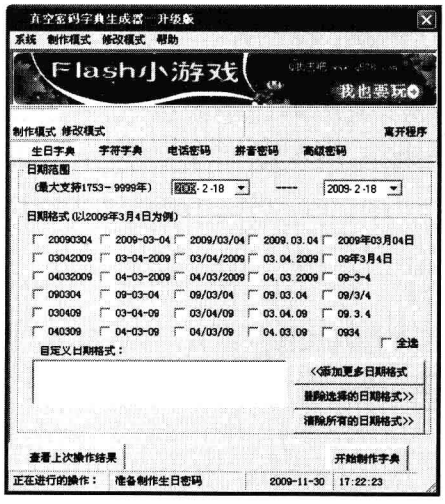



图 1-3　字典破解方式

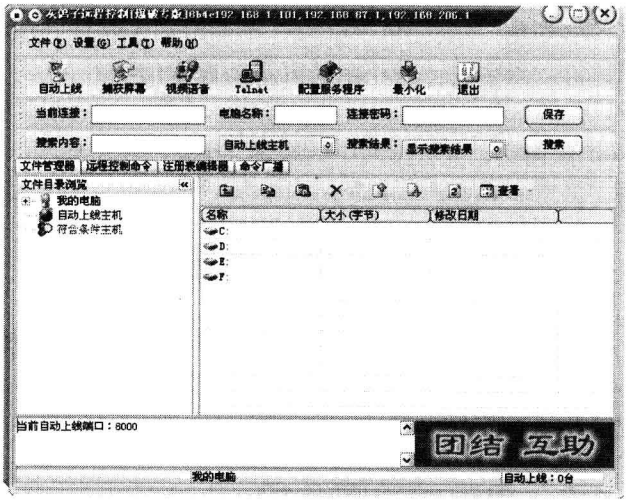



图 1-4　灰鸽子远程控制

### 4．缓冲区溢出攻击

缓冲区溢出攻击是指向程序缓冲区写入超出其边界的内容，造成缓冲区的溢出，使得程序转而执行其他攻击者指定的代码。攻击者通常使用该方法打开远程连接的 ShellCode，以达到攻击目的。著名的蠕虫病毒就是通过缓冲区溢出攻击获得系统权限后进行传播的。

### 5．网络监听

这是很多攻击前获取信息的一种途径，方式灵活多样，其实也是黑客攻击成功与否的关键步骤，因为黑客知道攻击目标的信息越多，攻击成功的概率也越高。

一般来说，网络监听分为嗅探器、混杂模式监听和共享式网络监听。其中嗅探器方式最为普遍，因为网卡的工作模式由操作系统设置，并没有公开的让用户进行设置的界面，而嗅探器的出现打破了这一僵局，使用户拥有了设置网卡工作模式的权利。这种嗅探方式是利用了计算机的接

口截获目的地为其他计算机发送的数据报文的一种工具，著名的工具有 IRIS、Ethereal 等。


**应该注意到，入侵的手段其实万变不离其宗，都是漏洞性的侵入作为前提，所以对于个人用户来说，及时地升级系统、安装杀毒软件和防火墙是十分必要的。**

上面介绍了几种常见的入侵手段，而防护方式，大概分为以下几类：

**1．ping 检测**

如果怀疑某台计算机在进行监听，可能像网络发送大量的垃圾数据包，这时网络的反应会非常慢，通过对比分析，可以监听到发起攻击的源头。

**2．使用反监听软件**

可以使用反监听软件来侦测监听者，比如 antisniffer 等。

**3．ARP 数据包检测**

ARP 数据包检测非常实用，如果怀疑有非法入侵者，采用 ARP 方式对 MAC 地址和 IP 地址进行绑定后，那些非法入侵者就原形毕露了。

**4．补丁升级**

对于每天都有新的漏洞的系统来说，打补丁至关重要。纵然你有再高超的技术，如果对方利用了操作系统漏洞，再先进的技术也显得苍白无力，毕竟，计算机的所有程序是运行在操作系统上的。

**5．反病毒软件**

反病毒软件主要针对木马等病毒，各个杀毒软件各有利弊，这里不做特别推荐，但不管使用哪款杀毒软件，都要记得及时升级病毒库。

**6．良好的操作习惯**

这是非常重要的一点，不浏览不健康网站，会让计算机保险系数更高，被黑客盯上的概率更小。

## 1.1.4 黑客工具亮一亮

一般来说，从黑客入侵流程来看，使用工具大体分为以下几种类型：

**1．扫描工具**

扫描工具是一种可以快速查找到目标计算机系统漏洞和弱点的工具。黑客可以根据扫描工具提供的漏洞信息有针对性地对目标发出攻击。

这种软件一般都是黑客行动的前期探路工具，毕竟在茫茫互联网中，还存在着很多有漏洞的主机，当然也可以针对某个 IP 地址进行扫描，比如通过一些方法，知道了对方的 IP 地址，通过扫描以后，就可以知道对方计算机中是否含有漏洞，以方便进一步入侵。

**2．破解工具**

如果扫描成功以后，无法通过溢出等方式获取管理员权限，就需要采用破解工具。黑客入侵计算机时往往需要多次输入账号和密码，除了采用猜测法来猜测账号和密码外，采用专门的破解软件可以快速破解出对方的账号和密码。

### 3．控制工具

木马绝对是这类工具的代名词，木马是程序员编写的一种恶意远程控制程序。当木马被植入目标计算机后，它会在未经用户许可的情况下，记录用户键盘输入的信息，盗取用户的各种账户和密码等信息，并将其发送给木马植入者。

### 4．攻击工具

使用这类工具时，黑客不一定要控制对方，而是想通过攻击来破坏对方网络或计算机的正常运行。最为熟悉的就是拒绝服务攻击，即 DoS 攻击，通过发送大量的终端数据，让对方网络忙不过来以致无法响应。


这里提到的 DoS 攻击，并不是指操作系统 DOS，DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，目前没有很好的方式解决这种攻击。

### 5．扫尾工具

这类工具一般包括添加隐藏账号和后门、清除入侵遗留下的痕迹、建议新漏洞等功能的软件，这是为了更好地保护“肉鸡”以便下次更方便地入侵。


这里说的“肉鸡”是指电脑“肉鸡”，就是拥有管理权限的远程电脑，也就是受别人控制的远程电脑。最早所说的“肉鸡”是一台开了 3389 端口的电脑，现在更多是指被木马控制的计算机。

## 1.2 黑客命令

本节所说的黑客命令，并不是指一款具体的软件，而是指黑客在进行通行操作时经常使用的网络命令。这些命令都是在命令提示符下完成的，进入命令提示符操作界面的步骤如下：

**步骤 1** 打开“开始”菜单，选择“运行”命令（如图 1-5 所示）。

**步骤 2** 在弹出的界面中输入 cmd 后按[Enter]键（如图 1-6 所示）。

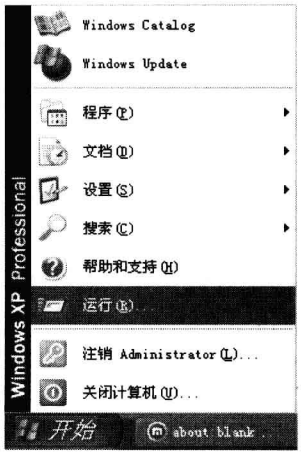



图 1-5 选择“运行”命令


图 1-6 输入 cmd 命令

**步骤 3** 打开命令提示符操作界面，默认显示当前用户名文件夹（如图 1-7 所示）。

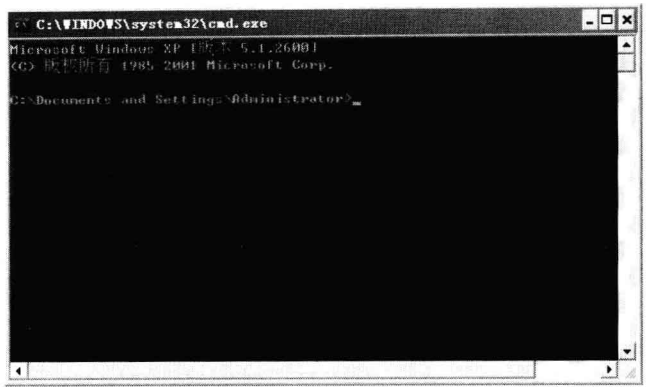



图 1-7　命令提示符操作界面

## 1.2.1　ping 命令

ping 命令是黑客入侵的基础命令，更是网络命令里的核心命令，在了解 ping 命令之前，需要先了解一下什么是 IP 地址。

IP 地址的全称是 Internet Protocol Address，所谓 IP 地址就是给每个连接在互联网上的主机分配的一个 32bit 地址。用户可以指定一台计算机具有多个 IP 地址，因此在访问互联网时，不要以为一个 IP 地址就是一台计算机；另外，通过特定的技术，也可以使多台服务器共用一个 IP 地址，这些服务器在用户看起来就像一台主机似的。

同样的，当访问某些网址的时候，实际上也是在访问一个 IP 地址，只不过 IP 地址不易记忆，所以才有了形形色色的网址。如果 ping 一下这个网址，就会看到它的真实地址了，比如在命令提示符提示符下输入 ping www.baidu.com 后按[Enter]键，结果如图 1-8 所示。

其中 202.108.22.43 就是访问网址的实际 IP 地址，后面的 time 显示返回时间，ping 最多等待 1 秒，TTL 值大小可以判断对方主机的系统类型。一般情况下，Windows 系列的系统返回的 TTL 值在 100～130 之间。

可以通过 ping 命令来检测与对方主机是否能够连通，如果返回的结果如图 1-8 所示，则表示连接正常，如果显示 Request timed out（见图 1-9），则表示无法正常连接。

图 1-8　Ping 网址

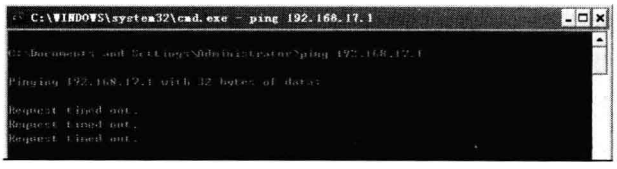



图 1-9　无法正常连通


有时由于网络问题，ping 命令可能迟迟没有反应，可以随时按下[Ctrl+C]组合键中断。



此为试读，需要完整PDF请访问：www.ertongbook.com