- 10小时维修专家实战教学视频（含电脑组装、维修、系统安装重装、故障排除等）
- 黑客攻防技术电子书
- 电脑常见软件故障处理电子书

创客诚品 编著

黑客攻防

从入门到精通

全新精华版

前沿网络安全工程师，
长达20年的安全维护经验，
适合初学者的黑客攻防宝典！

攻防技术+安全防护+数据还原一本通，
懂得黑客攻击手段，才能深入掌握防御技能！

243个网络安全知识 / 138个黑客攻防实战 / 28个备份与还原技巧

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

创客诚品

创客诚品 编著

黑客攻防

从入门到精通

全新精华版

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

创客诚品

内 容 简 介

本书从易到难、循序渐进且全面介绍黑客攻防的主要知识，涵盖了黑客攻防前的准备工作、扫描与嗅探攻防、Windows 系统漏洞攻防、密码攻防、病毒攻防、木马攻防等内容。书中内容丰富全面，图文搭配，深入浅出的讲解非常适合广大网络初学爱好者、从事网络安全的工作者及网络管理人员。

本书结构合理、案例详实，详细介绍了黑客攻防的基础知识与实际运用，旨在帮助提高读者网络安全意识与防御手段。

图书在版编目（CIP）数据

黑客攻防从入门到精通 / 创客诚品编著 . -- 北京 : 北京希望电子出版社 , 2017.11

ISBN 978-7-83002-543-4

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

中国版本图书馆 CIP 数据核字 (2017) 第 218068 号

出版： 北京希望电子出版社
地址： 北京市海淀区中关村大街 22 号 中科大厦 A 座 9 层
邮编： 100190
网址： www.bhp.com.cn
电话： 010-82620818（总机）转发行部
010-82702675（邮购）
传真： 010-62543892
经销： 各地新华书店

封面： 多　多
编辑： 全　卫
校对： 王丽锋
开本： 787mm×1092mm 1/16
印张： 20
字数： 474 千字
印刷： 固安县京平诚乾印刷有限公司
版次： 2018 年 5 月 1 版 2 次印刷

定价： 49.90 元

前言

Foreword

现在电脑、网络已经成为人们日常工作、学习、娱乐必不可少的工具。随着依托互联网的设备越来越多地出现在人们周围，安全问题日益突显。本书以黑客的角度分析电脑存在的各种安全问题，并结合笔者多年从事网络安全工作的经验，为读者讲解提高电脑网络安全性的方法。

写作目的

本书从黑客的角度出发，分析电脑及网络中存在的各种安全隐患，并讲解黑客如何利用这些漏洞达到破坏、控制、窃取目的的过程及技术手段。

本书并不是单纯地讲解各种黑客技术，而是通过研究黑客的入侵方式及手段，来分析电脑及用户操作存在的各种安全问题，以及解决这些问题的方法，从而增强用户的电脑安全防范意识，提高防范黑客入侵的手段及技术，降低黑客入侵成功率，减少损失。

章节导览

本书从认识黑客及黑客的基础知识讲起，讲解了黑客常用的攻击手段，以及如何防范黑客的攻击，其中各章内容介绍如下：

	章　节	概　要
基础知识	Chapter 01 ~ Chapter 02	认识黑客、常用命令、测试平台的搭建
入侵准备	Chapter 03	扫描及嗅探
入侵攻防	Chapter 04 ~ Chapter 08	系统漏洞、密码攻防、病毒攻防、木马攻防、后门攻防
综合攻防	Chapter 09 ~ Chapter 10	局域网攻防、远程控制
常用攻防	Chapter 11 ~ Chapter 13	QQ 攻防、上网及电子邮件攻防、网络设备安全
系统安全	Chapter 14 ~ Chapter 15	安全设置、备份与还原

写作特色

1. 涉及面广、触类旁通。本书将黑客最常用的攻击手段、入侵方法、入侵方式呈现在读者面前，不仅包含了一般的入侵步骤讲解，而且就一些常用软件、综合型的平台入侵实例进行了详细讲解。在讲解过程中，也对入侵的原理进行了介绍，使读者可以举一反三，触类旁通。

2. 侧重平衡、循序渐进。本书并不是单纯地讲解黑客入侵方法，而是通过黑客的角度，了解电脑及网络中的各种安全问题。在介绍了入侵后，会为读者讲解该入侵的防御手段，并且介绍了最实用的提升电脑安全性的方法。

3. 注重实际、通俗易懂。本书在讲解理论之后，通过大量实例，讲解入侵的过程。并通过介绍平台的搭建，使读者可以通过单机模拟显示的局域网环境，将理论直接运用到实际环境中，帮助读者快速掌握及运用所学知识。

编　者

目录

CONTENTS

Chapter 01

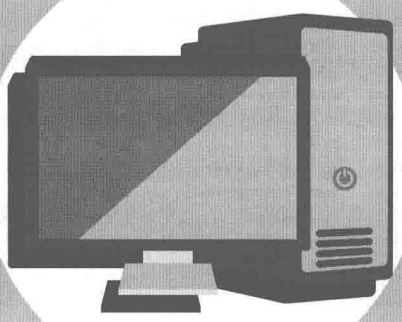
认识黑客

知识概述

古语云，知己知彼方能百战百胜。本书对黑客及黑客技术进行介绍，目的是帮助读者增强计算机安全防范意识，提高防范黑客入侵的手段及技术。本章将重点介绍黑客的相关概念、黑客的目标、主要入侵方式、被黑后的表现以及黑客常用命令。

要点难点

- 黑客的概念
- 黑客的术语
- 黑客的攻击手段
- 黑客常用命令



1.1 黑客的概念

计算机自从诞生以来，黑客就与其相伴相生。对于黑客，其实一直不曾有明确的定义。有人把黑客当做好奇心驱使的探险者，另一些人则把黑客当做恶意满满的破坏者。

“黑客”一词是由英语Hacker音译而来的，是指专门研究、发现计算机和网络漏洞的计算机爱好者。他们伴随着计算机和网络的发展而成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，不断发现计算机和网络中存在的问题，喜欢挑战高难度的网络系统并从中找到漏洞，然后找出解决和修补漏洞的方法。

1.1.1 黑客与骇客

“黑客”大体上分为“正”“邪”两类。正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并进行修补，而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络安全的事情。因为邪派黑客所做的事情违背了《黑客守则》，所以他们真正的名字叫“骇客”（Cracker），而非“黑客”（Hacker）。

无论哪类黑客，他们需要掌握的基础知识和基本技能都是一样的，只不过动机不一样而已。

黑客并不是只会使用几种简单的工具，从职业角度来说，黑客需要具备以下几种基本条件。

1. 了解一定量的英文

学习英文对于黑客来说非常重要，因为现在大多数资料和教程是英文版的，而且有关黑客的最新资讯也是从国外传进来的。一个漏洞从发现到出现中文介绍，需要大约一星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当用户看到中文介绍的时候，这个漏洞可能早就不存在了。因此，黑客从一开始就会尽量阅读英文资料，使用英文软件，并且随时关注国外著名的网络安全网站。

2. 学会基本软件的使用

这里所说的基本软件是指两种：一种是各种电脑常用命令，如ftp、ping、net等；另一种黑客工具，主要包括端口扫描器、漏洞扫描器、信息截获工具、密码破解工具等，如图1-1所示。这些软件的品种多，功能各不相同，后面将会介绍几款流行的黑客常用软件，在掌握其基本原理后，既可以选择适合自己的，也可以进行开发创造，进而编写自己的黑客工具。

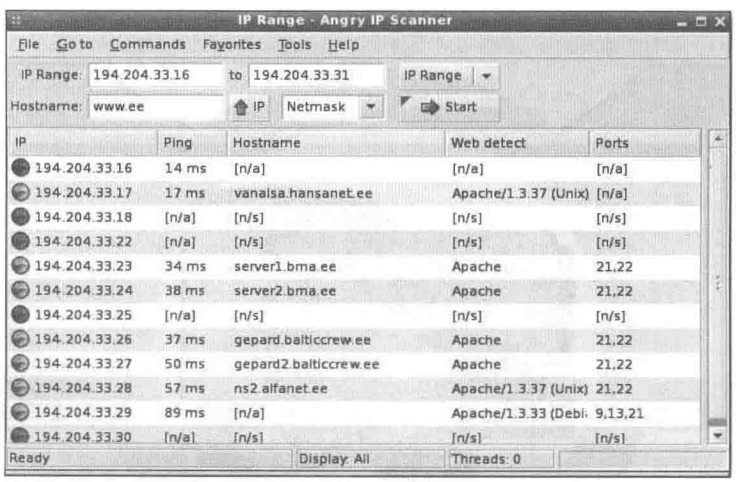


图1-1 IP及端口扫描工具

3. 对常见操作系统有深入的研究

常见的操作系统有Windows XP、Winodws 7、Windows 8、Windows 10等桌面系统，以及Windows Server等服务器系统，如图1-2所示。还有Unix及基于Linux的桌面及服务器系统。

黑客需要了解系统的常见漏洞，懂得这些系统的安全配置，并有一定的使用心得。

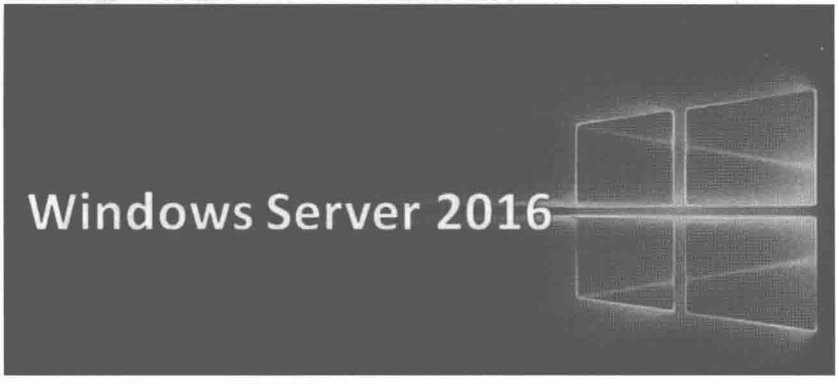


图1-2 Winodows Server 2016

4. 了解网络协议和工作原理

需要“按照自己的理解方式”弄明白网络的工作原理。因为协议涉及的知识多且复杂，如果在一开始就进行深入研究，势必会大大挫伤学习积极性。在这里建议，初步了解TCP/IP协议，如图1-3所示，包括浏览网页的时候网络是如何传递信息，客户端浏览器如何申请“握手信息”，服务器端如何“应答握手信息”并“接受请求”等内容。

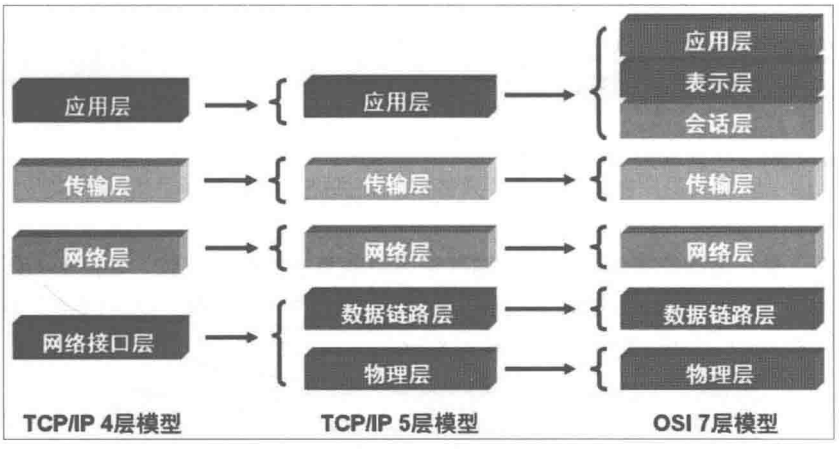


图1-3 OSI模型及TCP/IP对应关系

5. 熟悉几种流行的编程语言和脚本

建议初步学习C语言、ASP和CGI脚本语言，对HTML超文本语言、PHP、Java等有基本了解，主要学习这些语言中的“变量”和“数组”部分。因为语言之间存在内在联系，所以只要熟练掌握其中一门，其他语言基本上可以触类旁通。

6. 熟悉网络应用程序

网络应用程序包括各种服务器软件后台程序，例如wuftp、Apache等服务器后台；还有网上流行的各种论坛、电子社区。有条件的读者将自己的电脑做成服务器，如图1-4所示，然后安装并运行一些论坛代码。经过一番尝试之后，将会感性地理解网络工作原理，这比依靠理论学习要容易许多，能够达到事半功倍的效果。

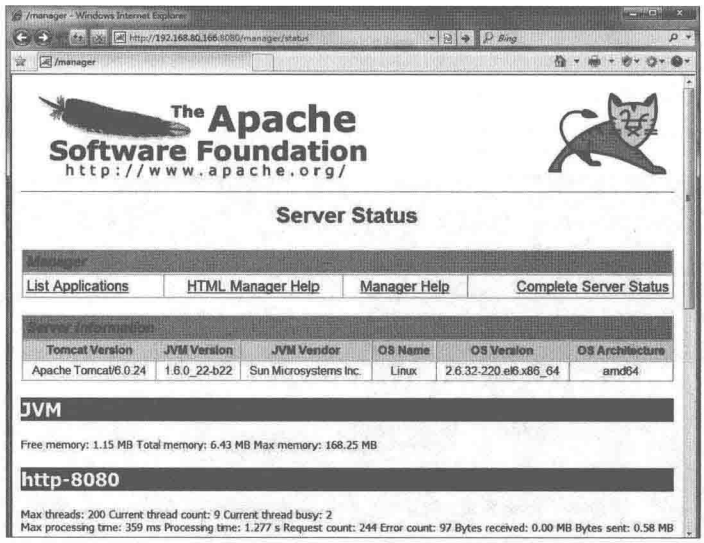
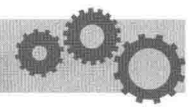


图1-4 Apache与TomCat组合的Web服务器

1.1.2 红客

红客（Honke）是一种精神，一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神并热爱计算机技术的“黑客”都可称为红客。红客通常会利用自己掌握的技术维护网络安全，并对外来的进攻进行还击。

1.2 黑客主要术语



本节将对常见的一些黑客术语进行介绍。

1. 肉鸡

所谓“肉鸡”是一种很形象的比喻，比喻那些可以随意被控制的电脑，如图1-5所示。对方可以是Windows系统，也可以是Unix/Linux系统，可以是普通的个人电脑，也可以是大型的服务器，可以像操作自己的电脑那样来操作它们，而不被对方察觉。

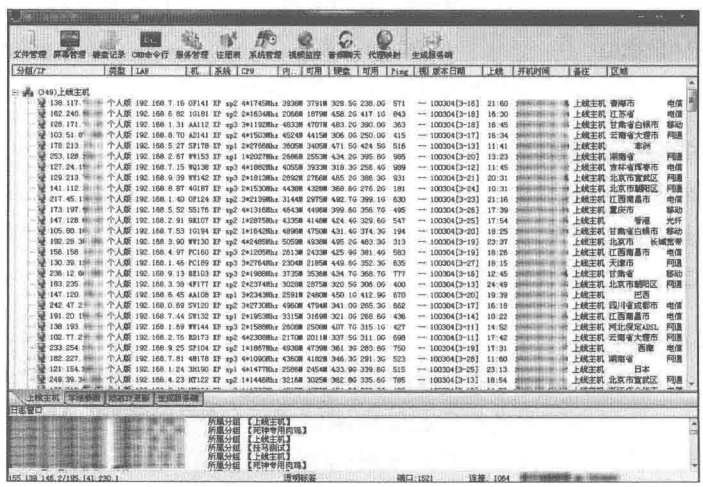


图1-5 黑客控制的大量肉鸡

2. 木马

木马是那些表面上伪装成正常程序的程序。当这些程序被运行时，就会获取整个系统的控制权限。很多黑客热衷于使用木马程序来控制别人的电脑，如灰鸽子、黑洞、PcShare等，如图1-6所示。

图1-6 灰鸽子远程控制客户端

3. 网页木马

网页木马表面上伪装成普通的网页文件，或是将自己的代码直接插入正常的网页文件中。当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上并自动执行。

4. 挂马

在别人的网站文件中放入网页木马，或是将代码潜入到对方正常的网页文件里，以使浏览者中马。

5. 后门

这是一种形象的比喻，入侵者用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动表面上是很难被察觉的，但是入侵者可以使用相应的程序或者方法来轻易地与这台电脑建立连接，重新控制这台电脑，就像是入侵者偷偷配了一把房间主人的钥匙，可以随时进出而不被主人发现。

6. rootkit

rootkit是攻击者用来隐藏自己的行踪和保留root（根权限，可以理解为Windows下的system或者管理员权限）访问权限的工具。通常，攻击者通过远程攻击的方式获得root访问权限，或者先使用密码猜解（破解）的方式获得对系统的普通访问权限，进入系统后，再通过对方系统内存在的安全漏洞获得系统的root权限。然后，攻击者就会在对方的系统中安装rootkit，以达到长久控制对方电脑的目的。rootkit与木马和后门类似，但远比它们隐蔽得更好，黑客守卫者就是典型的rootkit，还有国内的ntroorkit也是不错的rootkit工具。

7. IPC$

IPC$即共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机共享资源时使用。

8. 弱口令

弱口令指那些强度不够，容易被猜解的口令，如123、abc这样的口令或密码。

9. 默认共享

默认共享是指Windows系统开启共享服务时自动开启所有硬盘的共享，因为加了$符号，也称为隐藏共享。

10. shell

shell指的是一种命令执行环境。比如，按下键盘上的“开始键+R”时，出现“运行”对话框，在里面输入cmd，会出现一个用于执行命令的窗口，这就是Windows的shell执行环境。通常，使用远程溢出程序成功溢出后得到的用于执行系统命令的环境就是对方的shell。

11. 溢出

确切地讲，应该是“缓冲区溢出”。简单地解释，溢出是指程序对接受的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。大致可以分为两类：堆溢出与栈溢出。

12. 注入

随着B/S模式应用开发的发展，使用这种模式编写程序的程序员越来越多，但是由于程序员的水平参差不齐，相当多的应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些想知道的数据，这就是所谓的SQLinjection，即SQL注入。

13. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库的运行帐号的权限的不同，所得到的权限也不同。

14. 端口（Port）

端口相当于一种数据的传输通道。用于接受某些数据，然后传输给相应的服务，计算机将这些数据处理后，再将相应的服务通过开启的端口传给对方。一般，每个端口的开放对应相应的服务，要关闭这些端口，只需要将对应的服务关闭就可以了。如图1-7所示，可以查看当前计算机使用的端口信息。

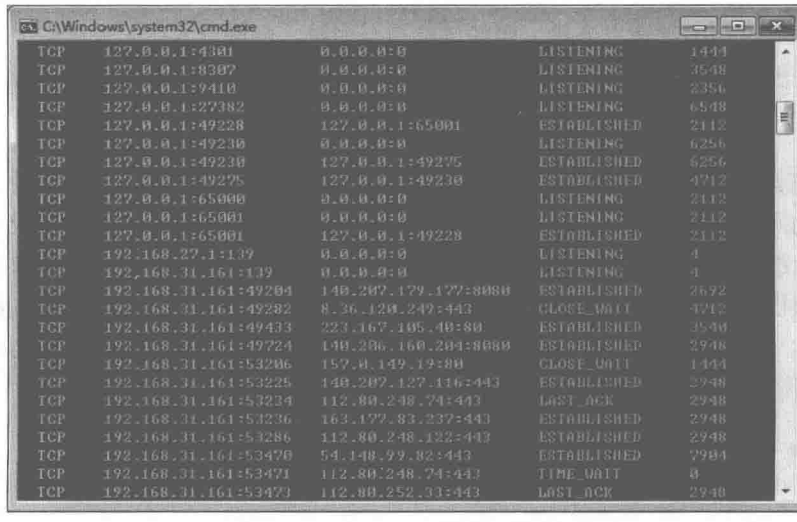


图1-7 查看当前计算机使用的端口

15. 免杀

免杀就是通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16. 加壳

加壳是利用特殊的算法，将EXE可执行程序或者DLL动态连接库文件的编码进行改变（如压缩、加密），以缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀。目前较常用的壳有UPX、ASPack、PePack、PECompact、UPack、免疫007、木马彩衣等，如图1-8所示。

17. 花指令

花指令是几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常判断病毒文件的构造。杀毒软件是从头到脚按顺序来查找病毒的，如果把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。如图1-9所示为免杀花指令生成器。

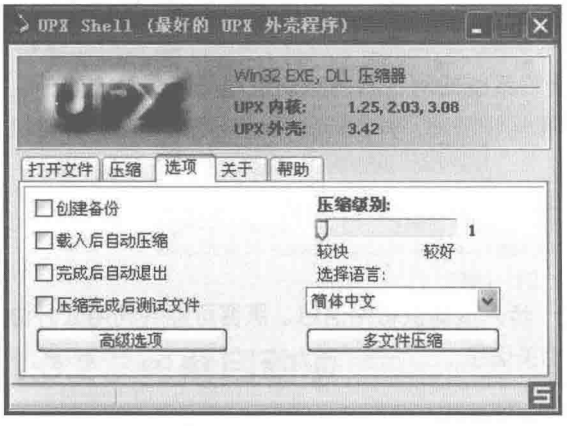


图1-8 UPX加壳工具

图1-9 免杀花指令生成器

18. 协议

网络是一个信息交换的场所，所有接入网络的电脑都可以通过彼此之间的物理连接设备进行信息交换。这种物理设备包括最常见的电缆、光缆、无线、微波等，但是单纯拥有这些物理设备并不能实现信息的交换，信息交换还要具备软件环境。这种“软件环境”是人们事先规定好的一些规则，被称作“协议”。有了协议，不同的计算机可以遵照相同的协议使用物理设备，并且不会造成相互之间的“不理解”。电脑通过各种预先规定的协议完成不同的使命，例如RFC1459协议可以实现IRC服务器与客户端电脑的通信。因此无论是黑客，还是网络管理员，都必须通过学习协议了解网络运作的机理。每个协议都是经过多年修改延续使用至今的，新产生的协议也大多是在基层协议基础上建立的，因而协议具有相对较高的安全机制，黑客很难发现协议中存在的安全问题。但是对于某些新型协议，因为出现时间短，考虑欠周到，也可能会因安全问题而被黑客利用。

19. 服务器与客户端

最简单的网络服务形式是：若干台电脑做客户端，使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端。这样的协议很多，如平时接触的电子邮件服务器、网站服务器、聊天室服务器等都属于这种类型。还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端进行连接，也就是说每一台电脑既是服务器，又是客户端，它们之间具有相同的功能，对等地完成连接和信息交换工作，DCC

传输协议就属于此种类型。由此看出，客户端和服务器分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，都是操作自己的电脑（客户端），并且向网络服务器发出常规请求，完成浏览网页、收发电子邮件等任务。黑客则是通过自己的电脑（客户端）对其他电脑（有可能是客户端，也有可能是服务器）进行攻击，以达到入侵、破坏、窃取信息的目的。

20. 漏洞

漏洞是程序中没有考虑到的情况。例如，最简单的“弱口令”漏洞是指系统管理员忘记屏蔽某些网络应用程序中的帐号；Perl程序漏洞则可能是因设计程序的时候考虑情况不完善而出现的“让程序执行起来不知所措”的代码段；“溢出”漏洞则属于当初设计系统或者程序的时候，没有预先保留足够的资源，而在日后使用程序时造成的资源不足；特殊IP包炸弹实际上是程序在分析某些特殊数据的时候出现错误。总而言之，漏洞就是程序设计中的人为疏忽，这在任何程序中都无法绝对避免，黑客也正是利用种种漏洞对网络进行攻击的。

1.3 黑客入侵及异常表现

对于红客或者善意黑客来说，在侵入目标后，会将系统或网络漏洞告知管理员以便及时修补。对于恶性黑客或者骇客来说，在侵入目标后，会盗取帐号、密码，并制造恶作剧或炫耀高超的计算机技术。

下面将对黑客入侵的大致流程进行介绍。

1. 收集网络系统中的信息

收集信息，并且不会对目标产生危害，只是为进一步入侵提供有用信息。黑客可能会利用公开协议或工具，收集驻留在网络系统中的各个主机系统的相关信息。

2. 探测目标网络系统的安全漏洞

在收集到攻击目标的一定量信息后，黑客会探测目标网络上的每台主机，并且寻求系统内部的安全漏洞。

3. 建立模拟环境，进行模拟攻击

根据前面所得的信息，建立一个类似攻击对象的模拟环境，然后对此模拟目标进行一系列的攻击。在此期间，通过检查被攻击方的日志，观察检测工具的攻击回馈信息，可以进一步了解在攻击过程中留下的“痕迹”及被攻击方的状态，以此来制定一个较为周密的攻击策略。

4. 具体实施网络攻击

入侵者根据前面获得的信息，同时结合自身的水平及经验总结出相应的攻击方法，在进行模拟攻击的实践后，等待时机，实施真正的网络攻击。

黑客入侵后，系统将会表现出不同程度的异状。

1.3.1 进程异常

按快捷键Ctrl+Alt+Del调出任务管理器，查看有什么进程在运行，如图1-10所示。如果发现陌生的进程，就要多加注意，可以先关闭一些可疑的程序，如果发现一些不正常的情况恢复了正常，那么就可以初步确定是中了木马了。发现有多个名字相同的程序在运行，而且还会随时间的增加而增多，这也是一种可疑的现象，也要特别注意。如果是在连入Internet或局域网后才发现这些现象的，需要