电脑报 总策划

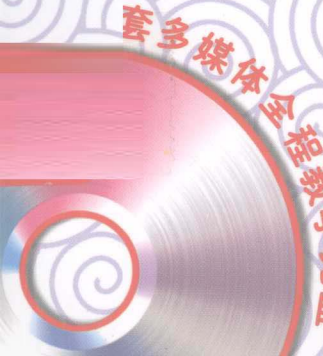
# 黑客入门

新手特训

## 精彩看点

- **实练特训 专为新手打造的入门级图书**
  手把手讲解，图解例说，一看就懂
  全程Flash互动教学光盘，助你快速掌握
- **黑客入侵前奏曲**
  扫描网络漏洞主机，锁定目标“肉鸡”
  嗅探报文数据，捕获机密资料
- **电脑密码加密解密**
  BIOS、Windows系统密码清除技巧
  Office文档、加密光盘解密实战
- **系统漏洞入侵与防范实战**
  基于IPC$、Telnet等认证入侵要略
  通过溢出漏洞提升权限

力行工作室 编




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

# 黑客入门新手特训

力行工作室　编

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

## 内容简介

本书从初学者的需求出发，精心组织了全新的内容，并以独特的编排方式呈现给广大读者，以期在短时间内达到最佳的学习效果；再辅以配套光盘中的多媒体教程的学习巩固，能让读者充分领会并快速了解黑客入侵的原理，从而高度重视网络安全，并采取相关措施现场自救。

全书从实用性和可操作性的角度出发，以图解的形式深入浅出地介绍了黑客的基本知识和攻击、防范的操作步骤，并对初学者在学习过程中经常遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路，全书内容包括：黑客基础知识、扫描、嗅探与欺骗、密码破解大揭密、利用Windows系统漏洞进行攻击、木马的植入、木马的清除与防范、QQ攻击大揭密、邮件欺骗与轰炸、恶意浏览器攻击、IIS服务器攻防、做好安全防范等内容。

警告：本书介绍的黑客技术仅供读者学习及预防，切勿攻击他人电脑，否则后果自负！



书　　名：黑客入门新手特训
作　　者：力行工作室
技术编辑：何　磊
封面设计：CCC工作室
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：四川省蓥山数码科技有限公司
文本印刷：重庆市联谊印务有限公司
开本规格：787mm×1092mm 1/16　15.5印张　300千字
版　　号：ISBN 978-89476-008-1
版　　次：2008年7月第1版　2008年7月第1次印刷
定　　价：29.80元(1CD+配套书)

# 零起点，快易通

## 前言 FORE

当你拿起这本书的时候，或许你已经将自己加入到电脑操作的新手行列，并且想快速地把握电脑应用的秘笈，那么本丛书正是为你量身定做的：如果你由于工作的关系没有时间去培训班学习；如果你正在面临考试；如果你还在单位处于试用阶段；如果在你使用电脑时遇到困难还无从着手；如果你到目前为止还没有更好地掌握电脑操作，那么就请相信你现在的选择，我们精心编写的这套《新手特训》系列丛书就是专门为你量身定制，它将帮助你快速从入门到精通。

本丛书具有以下五大特色：

**◆互动教学，书盘合一**

全新的Flash互动教学光盘，对书中所涉及到的主要知识点给予了全面的解读，进一步提高你的学习兴趣；如果你不喜欢长时间阅读书籍，本丛书光盘也能够满足你的学习需求；超过2小时的教学内容，为你快速成长提供了有力的保障。特别需要指出的是，它更可以作为培训的多媒体课程。

**◆立足新手，实练特训**

本丛书充分从新手的角度考虑问题，想新手之所想，做新手之所需。所选择的内容均是相关领域应知应会的内容，在最大程度上使读者在最短时间内更快更好地掌握相关知识，每章后附有各类习题可以帮助读者及时消化本章知识，做到学练结合。

**◆图解例说，简明易懂**

考虑初学者的实际情况，本丛书基本做到一步一图，而且以图解的方式指导具体操作步骤，STEP BY STEP的写作方式更能帮助读者对每一个操作步骤透彻理解。

**◆双栏排版，双色印刷**

在版面的设计上，我们特意选择了双栏编排，不仅增加了知识的容量，而且为读者降低了购买成本。与黑白印刷相比，双色图书具有直观、鲜明的特点，同时可以避免阅读疲劳，能够让读者高效、快速理解相应的电脑操作。

**◆结构合理，内容适度**

电脑的每一个领域其实都有着深奥的知识，作为新手的你究竟该掌握哪些相关知识呢？作为初学者阅读的书籍，在内容的选择上我们均经过认真讨论，反复研究，尽可能在丰富内容的基础上，取其精华，去其糟粕，以使读者在最短的时间内掌握真正所需要的知识。

电脑报

2008.7

# 多媒体光盘教程要目

MULTIMEDIA COMPACT DISC DIRECTORY

本光盘与图书内容一一对应，采用全程语音讲解、情景式教学，详细的图文对照和真实的操作演示，可帮助读者轻松掌握操作要领，提高学习效率。

在主界面选择要观看的栏目，点击相应的内容即可播放。以下为多媒体教程索引：




特别感谢：本书多媒体教程由成都登巅资讯制作。

# 练习题答案

## 第1章

### 一、填空题

1. Hacker　是指专门研究、发现计算机和网络漏洞的计算机爱好者。

2. 目标信息系统　弱点信息挖掘分析　目标使用权限获取　开辟后门

### 二、简答题

略

### 三、练习题

略

## 第2章

### 一、选择题

1.A

2.ABC

### 二、填空题

1.数字加密、数字签名、公/私钥加密、证书

2.Back Door(后门)

3.利用数学算法　可理解形式的明文

### 三、简答题

略

## 第3章

### 一、选择题

1.B

2.C

### 二、填空题

1. 扫描

2. HTTP协议网络嗅探器、协议分析器、HTTP文件重建工具

3. 网络欺骗技术、端口重定向技术、攻击(入侵)报警和数据控制、数据捕获技术

### 三、问答题

略

## 第4章

### 一、选择题

1.A

2.D

### 二、填空题

1.安全缺陷

2.程序缓冲区编写超出其长度的代码

### 三、问答题

略

## 第5章

### 一、选择题

1.ABCDE

2.D

### 二、填空题

1.一段特定的程序(木马程序)　控制端　被控制端

2.控制端和服务端都要在线　服务端已安装了木马程序

### 三、问答题

略

## 第6章

### 一、选择题

1.ABCD

2.C

### 二、填空题

1.关闭无用端口　程序

2.子协议　　Ping　Tracert

### 三、问答题

略

## 第7章

### 一、填空题

1.本机　黑客手段

2.窗口函数

### 二、问答题

略

## 第8章

### 一、选择题

1.B

2.A

### 二、填空题

1.垃圾邮件

2.相似的电子邮件地址　　修改邮件客户远程登录到端口25

### 三、问答题

略

## 第9章

### 一、选择题

1.ABCDE

2.A

### 二、填空题

1.死循环　打开窗口死循环　超大图片　格式化硬盘

2.软件　系统操作平台　HTML超文本标记语言

### 三、问答题

略

## 第10章

### 一、选择题

1.A

2.B

### 二、填空题

1.应用程序日志　安全日志　系统日志　DNS服务器日志　FTP日志

2.Index Server　highlighted(突出)

### 三、问答题

略

## 第11章

### 一、选择题

1.ABCD

2.D

### 二、填空题

1. 漏洞　BUG的程序

2. 过滤型　检测型　代理型

### 三、问答题

略

# 目录

## 第1章 黑客基础知识

随着互联网技术的飞速发展，网络世界的安全性不断受到挑战。如果你要上网，就免不了遇到黑客的侵扰。本章就为大家介绍一些最基本的黑客入门知识，揭秘黑客常用的一些命令，当然这些微不足道的伎俩难以入侵戒备森严的网络，不过至少让初学者对黑客的“工作情形”有初步的认识。



## 第2章 扫描、嗅探与欺骗防范

黑客通常都是通过扫描探测来发现计算机的漏洞，本章主要介绍一些常用的扫描器、嗅探工具，最后介绍了网络欺骗。本章是黑客常用的手段，属于必备掌握的知识。

CONTENTS 目录

## 第3章 密码破解大揭秘

在对安全和保密需求日益增长的时代，有很多加密工具能够保护用户的信息安全，但是这些加密工具也受到密码破译的挑战。在忘记密码的时候，破解密码也是一个找回密码的途径。在本章中将介绍各个方面常用的密码破译方法和破译工具。



## 第4章 基于系统漏洞的入侵与防范

每个操作系统总是存在这样或那样的漏洞，对于这些漏洞，如果不加强防范，黑客就会利用系统的漏洞入侵电脑，甚至对一些分区进行格式化操作等危险操作。

## 第5章 基于木马的入侵与防范

木马，也称特伊洛木马，英文名称为Trojan。其本身就是为了入侵个人电脑才出现的，木马在电脑工作的时候是很隐蔽的，不会在电脑的屏幕上显示出任何痕迹。本章从木马的基本原理入手，进而了解木马的具体攻击过程，以做到有效地防范木马。



## 第6章 木马的清除与防范

正如上一章所讲述的那样，木马的危害极大，那么如何保护我们的电脑不受木马侵害呢？感染了木马之后又该采取怎样的补救措施呢？本章将对如何防范和清除木马做详细的介绍。

CONTENTS 目录

## 第7章 QQ盗号大揭秘

网络聊天使天南海北的朋友打破了地域的限制，可以和任何地方的朋友进行交流，方便了工作和生活。QQ是目前国内使用最广泛的网上聊天软件，所以针对QQ的攻击方法也比较多，本章将为读者介绍一些QQ被攻击的实例。如此我们就能有效地防范QQ被攻击了。



## 第8章 邮件欺骗与轰炸

电子邮件（E-mail）是现在网络的基本通讯工具之一，在人们的日常生活和工作中发挥着越来越大的作用。使用电子邮件的公司和个人也越来越多，电子邮件的安全性也成为了人们担忧的一个问题。本章介绍电子邮件的攻击和防范。

## 第9章 浏览器恶意攻击

Internet Explorer是使用最广泛的网页浏览器，由于它的功能强大，故支持JavaScript脚本、ActiveX控件等元素，这也使得它在浏览网页时留下了不少安全隐患。利用网页进行攻击是非常难以防范的，目前，大多数的防范方法是以损失很多浏览器功能为代价的。



## 第10章 IIS服务器的入侵与防范

本章主要介绍IIS常见的漏洞，详细讲述了IIS漏洞攻击和防范方法。通过本章的学习，读者可以掌握IIS漏洞的攻防相关知识。

## 第11章 安全防范黑客入侵

出色的黑客更应该注意防守，首先就是隐藏好自己的IP，关闭不必要的端口，然后再使用网络防火墙来防范攻击和限制木马程序的连接。本章主要介绍提高系统网络安全防御能力的通用方法。

# 第 1 章
# 黑客基础知识

重点讲解

- 什么是黑客
- 黑客攻击手法
- 黑客常用命令

随着互联网技术的飞速发展，网络世界的安全性不断受到挑战。如果你要上网，就免不了遇到黑客的侵扰。本章就为大家介绍一些最基本的黑客入门知识，揭密黑客常用的一些命令，当然这些微不足道的伎俩难以入侵戒备森严的网络，不过至少让初学者对黑客的“工作情形”有初步的认识。

本章导读

## 1.1 黑客简单介绍

最早的计算机于1946年在宾夕法尼亚大学出现，而最早的黑客出现于麻省理工学院（贝尔实验室也有）。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。

### 1.1.1 黑客的历程

1994年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会第三资源，它是未来生活中的重要介质。但是随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了。

### 1.1.2 黑客的由来

“黑客”一词是由英语“Hacker”英译出来的，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产生成长。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，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

黑客的出现推动了计算机和网络的发展与完善。他们所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上来讲，计算机的安全需要更多黑客去维护。这里我们借用黑客英雄网站长myhk的一句话：“黑客存在的意义就是使网络变得日益安全完善”。

但是到了今天，黑客一词已经被用于那些专门利用计算机进行破坏或入侵他人电脑的代言词，对这些人正确的叫法应该是Cracker，有人也翻译成“骇客”，也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，误认为黑客也是在网络上进行破坏的人。根据开放原始码计划创始人EricRaymond（埃里克.雷蒙德）的解释，Hacker与Cracker是分属两个不同世界的族群，基本差异在于，Hacker是有建设性的，而Cracker则专门搞破坏。

## 1.2 黑客入侵流程

黑客在进行攻击时通常有个习惯性的流程。首先搜寻到目标信息系统，然后找到目标信息系统的弱点，并利用弱点获得权限开辟后门，最后对痕迹进行清除。

### 1.2.1目标系统信息收集

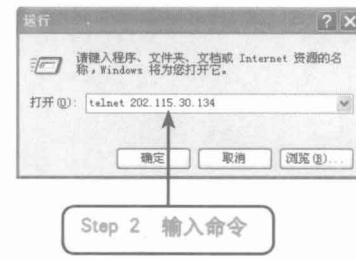
信息的收集并不对目标系统产生危害，只是为进一步的入侵提供有用信息。这些信息主要包括目标的操作系统类型及版本，目标主机提供哪些服务，各服务器程序的类型与版本以及相关的社会信息等。

要攻击一台机器，首先要确定它正在运行的操作系统版本。因为对于不同类型的操作系统，系统漏洞有很大区别，攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验，有些服务器的某些服务显示信息会泄露其操作系统。

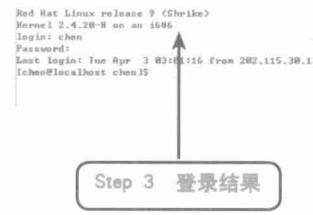
**【案例1-1】Telnet登录Linux服务器示例**

如果用户是在Windows的环境下，想对远程的Linux系统进行操作，推荐选择“telnet”的方式进行登录(telnet命令在后有详细的介绍)，具体步骤如下。


Step1　启动Windows操作系统，单击执行“开始”→“运行”命令。




Step2　弹出的“运行”对话框中输入“telnet+远程Linux系统IP地址”，例如：telnet 202.115.30.134。




Step3　弹出“RedHatLinux”界面，输入用户名和密码后，即可像在本机一样进行命令行的操作了，从图中可以得知该版本为Red Hat Linux release 9版本。

另外需要获得的信息就是一些与计算机本身没有关系的社会信息，例如网站所属公司的名称、规模，网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码，这就很容易被人试探出来。

信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快，可以一次对多个目标进行扫描。

### 1.2.2 弱点信息挖掘分析

在收集到一些准备要攻击目标的信息后，黑客们会探测目标网络上的每台主机，来寻求系统内部的安全漏洞，这些信息即所谓的弱点信息，主要探测的方式如下。

**1.自编程序**

对某些系统，互联网上已发布了其安全漏洞所在，但用户由于不懂或一时疏忽未打上该系统

的“补丁”程序，那么黑客就可以自己编写一段程序进入到该系统进行破坏。

#### 2.慢速扫描

由于一般扫描侦测器的实现是通过监视某个时间段里一台特定主机发起的连接的数目来决定是否在被扫描，这样黑客可以通过使用扫描速度慢的扫描软件进行扫描。

#### 3.体系结构探测

黑客利用一些特殊的数据包传送给目标主机，使其做出相对应的响应。由于每种操作系统的响应时间和方式都是不一样的，黑客利用这种特征把得到的结果与准备好的数据库中的资料相对照，从中便可轻而易举地判断出目标主机操作系统所用的版本及其他相关信息。

### 1.2.3目标使用权限获取

#### 1.获得权限

当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需利用工具发动攻击即可。而作为入侵性攻击，往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。有时获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力，这也符合黑客的追求。

能够被攻击者所利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理配置不当而造成的漏洞。

当然大多数攻击成功的范例还是利用了系统软件本身的漏洞。造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识。当攻击者对软件进行非正常的调用请求时，会造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出的攻击最为普遍，据统计80%以上成功的攻击都是利用了缓冲区溢出漏洞来获得非法权限的。

无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞。黑客需要用它来完成攻击，而管理员需要根据不同的漏洞来进行不同的防御措施。

#### 2.权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，如下图所示采用Norton杀毒软件漏洞扫描功能获取的系统安全漏洞的信息。远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始的。但是利用远程漏洞获取的不一定是最高权限，而往往只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。


只有获得了最高的管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。完成了权限的扩大后，不但可以利用已获得的权限在系统上执行利用本地漏洞的程序，还可以放一些木马之类的欺骗程序来套取管理员密码，这种木马是放在本地套取最高权限用的，而不能进行远程控制。

### 1.2.4开辟后门

黑客对目标主机进行了分析后，如果找到其弱点并打开了这台主机的后门，这时就可以向目标主机上传间谍程序了(通常黑客在目标主机上装上间谍程序后，会将IPC$连接断开，不然在会话中将留有记录)。

通过后门上传的间谍程序可以是做代理的跳板程序，也可以是扫描程序，还可以是嗅探器，这些程序通常都隐藏得很深。例如目标主机没有嗅探器，黑客就可以为其安装上Sniffer，用于监听FTP/POP3等的明文传输密码；如果目标主机开启了Web服务，那还可以给它安上一个脚本木马，脚

本木马如果放得好的话，检测难度非常大，而管理员在做Web备份的时候，也会把它备份进去，一个好的asp木马可以完全接管一台NT操作系统。然后把主机上有用的文件全部下载下来，如Web程序的数据库连接代码里会有数据库用户名和口令信息，可以利用后面章节中所讲的对MSSQL的入侵来完全控制主机。

### 1.2.5黑客常用手法

#### 1.口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，例如利用目标主机的Finger功能：当用Finger命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上；利用目标主机的X.500服务：有些主机没有关闭X.500的目录查询服务，也给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集：有些用户电子邮件地址常会透露其在目标主机上的账号；查看主机是否有习惯性的账号：有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号的泄露。

口令又有三种方法：

（1）通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法也是获取用户账户和密码的一条有效途径。当下，很多协议根本就没有采用任何加密或身份认证技术，如在Telnet、FTP、HTTP、SMTP等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到你的账户和密码。还有一种中途截击攻击方法更为厉害，它可以在你同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗你，再假冒你向服务器发出恶意请求，其造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的SUID程序来获得超级用户权限。

（2）在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但攻击者要有足够的耐心和时间。如：采用字典穷举法（或称暴力法）来破解用户的密码。攻击者可以通过一些工具程序，自动地从电脑字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把上十万条记录的字典里所有单词都尝试一遍。

（3）利用系统管理员的失误。在现代的Unix操作系统中，用户的基本信息存放在“password”文件中，而所有的口令则经过DES加密方法加密后专门存放在一个叫“shadow”的文件中。黑客们获取口令文件后，就会使用专门的破解DES加密法的程序来解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。

#### 2.放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在用户的电脑中，并在用户的计算机系统中隐藏一个可以在Windows启动时悄悄执行的程序。当你连接到因特网上时，这个程序就会通知攻击者，报告你的IP地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。