普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络攻防技术

武晓飞 主编
秦玉海 审

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

网络攻防技术

武晓飞 主编

Information Security

http://www.tup.com.cn

清华大学出版社

北京

内 容 简 介

本书主要面向网络安全技术初学者和相关专业学生。本书按照技术专题组织编写，第1章介绍网络安全基础知识，主要包括渗透测试平台BackTrack的基本内容和相关脚本语言的基本知识。第2～7章分别介绍了不同的网络攻防技术专题，主要包括信息收集技术、漏洞利用技术、密码破解技术、网络嗅探技术、Web应用安全和入侵防范与检测技术等。网络攻防技术的发展非常迅速，作为一门对实践能力要求很高的课程，本书非常注重提高学生的动手能力，精心选择了相关的网络安全工具软件，介绍了业界流行的渗透测试平台BackTrack的相关内容。对于每个网络攻防技术专题，本书都通过实例分析和详细的步骤讲解，力求把理论知识应用到实践中去。

图书在版编目(CIP)数据

网络攻防技术/武晓飞主编. --北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-35088-0

Ⅰ. ①网… Ⅱ. ①武… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第009186号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：时翠兰
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：5.5　　**字　　数**：122千字
版　　次：2014年11月第1版　　**印　　次**：2014年11月第1次印刷
印　　数：1～2000
定　　价：19.50元

产品编号：056297-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

为了适应教学需求，课程组的老师们对网络攻防的基本理论知识、流行的安全工具进行了整理和组织，结合相关的课程授课经验，决定以专题式、实例式的形式来编写此书，希望学生通过具体实践来解决任务挑战，提高实战技能，更加深入地理解网络攻防理论知识和技术原理。

本书的第1章主要介绍网络攻防的基础知识，要求学生了解和掌握利用虚拟机来搭建实验环境的方法和步骤，并且学会利用数据包捕获工具对攻防过程进行必要的分析和取证。通过引入业界流行的渗透测试平台 BackTrack，使学生了解前沿的技术工具和攻防手段。为了更好地理解和掌握后续章节中出现的案例和代码，在第1章中还介绍了 Linux Bash 脚本和 Python 脚本的基础知识。

从第2章开始，分别介绍网络攻防领域中不同的技术专题。通过作者自主设计和网上借鉴的实例式任务，引导学生主要利用 BackTrack 中的开源或免费软件工具，在攻防实验环境中锻炼实践能力，达到提高实战技能的目的。对于一些实例任务，不但要求学生会用工具软件来完成，甚至还要求通过更高的技术手段，比如自己编写脚本代码，来解决任务挑战。

全书共有7章，其中第1～4章由武晓飞编写，第5章由徐国天编写，第6章由段严兵编写，第7章由肖萍和郭睿编写。

由于作者水平有限，书中难免存在疏漏或不足之处，欢迎使用本书的师生提出宝贵意见。

编　者

2014年9月

目录

第1章 网络攻防基础

本章的主要内容包括 BackTrack5 的基本介绍和 Bash、Python 等脚本语言的基础知识。

1.1 BackTrack 基础

BackTrack 基于 UBUNTU 操作系统，预先安装了很多网络安全工具。本节主要介绍在虚拟机中安装 BT5 的方法和步骤以及 BackTrack 提供的一些常用网络服务的使用方法。

1.1.1 BT5 的虚拟机安装

在 BackTrack 的官方网站上(http://www.backtrack.org)提供 BT5 的下载，并且提供了一些下载选项。

如图 1-1 所示，可以选择是下载 32 位系统还是 64 位系统，可以选择镜像文件的类型是 ISO 文件还是可以用虚拟机直接打开的文件，可以选择 BT5 的桌面系统是 GNOME 还是 KDE，以及下载的方式是直接下载还是通过 Torrent 种子文件下载。

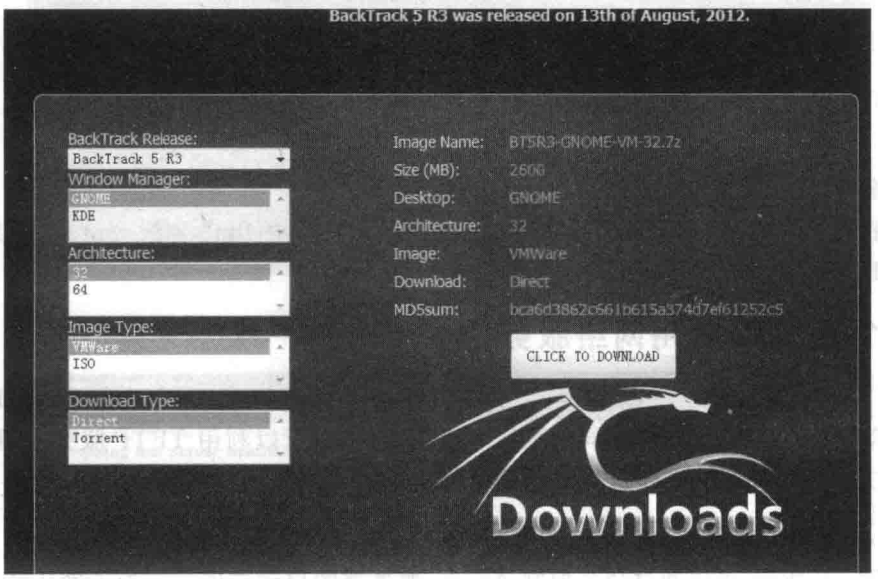

图 1-1 BT5 下载选项

假设下载了32位的虚拟机类型文件，得到的是一个压缩文件包，解压缩后存放在一个硬盘目录中，接下来就可以直接使用虚拟机软件，比如用VMWare Player或者Virtual Box打开BT5。

步骤1：在VMWare Player虚拟机的主界面中单击“打开虚拟机”，如图1-2所示。

图1-2　使用VMWare Player打开BT5虚拟机

步骤2：选中相应目录下的文件，如图1-3所示。

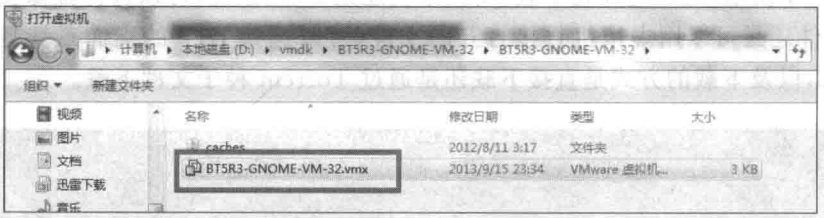

图1-3　选择虚拟机文件

步骤3：启动BT5虚拟机，如图1-4所示。

虚拟机启动后，进入登录界面，如图1-5所示。默认的用户名是root，密码是toor。进入BT5系统后，可以利用startx命令启动图形界面。

1.1.2　BT5常用网络服务

BT5中可以方便地启动各种网络服务程序，比如HTTPD、SSHD、TFTPD、VNC Server等。它们可以应用在不同的测试环境中。例如，可以利用TFTP服务向目标机传输木马文件，可以利用SSH进行远程登录等。

1. Apache服务

如图1-6所示，可以通过命令控制Apache服务器的启动或停止。为了确认Apache服务器已经开启，可以使用netstat命令来查看。

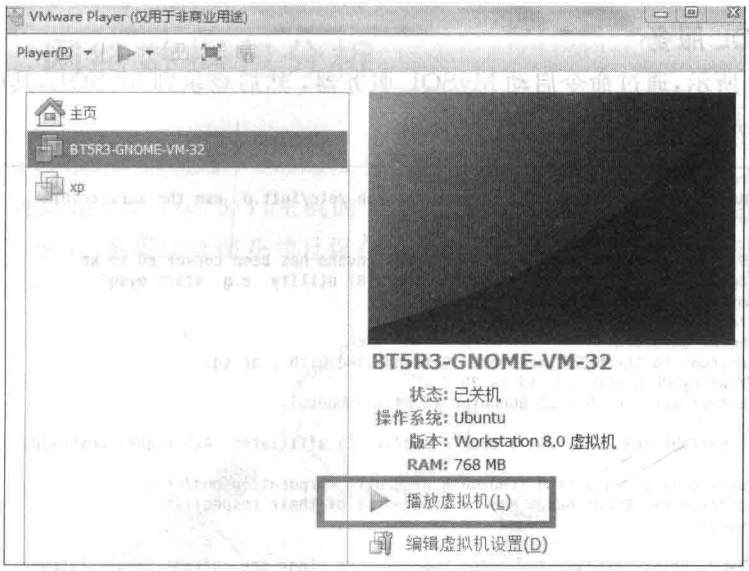

图 1-4　启动 BT5 虚拟机

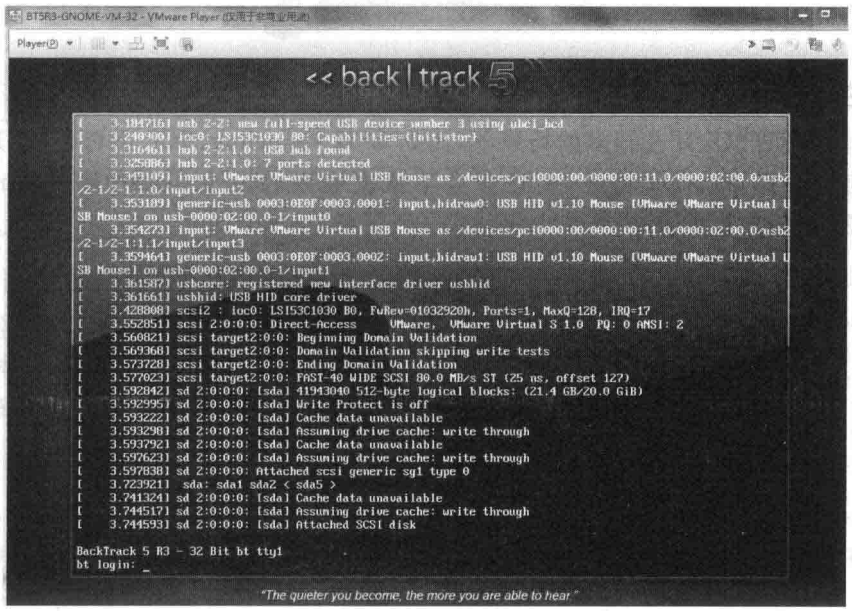

图 1-5　BT5 登录界面

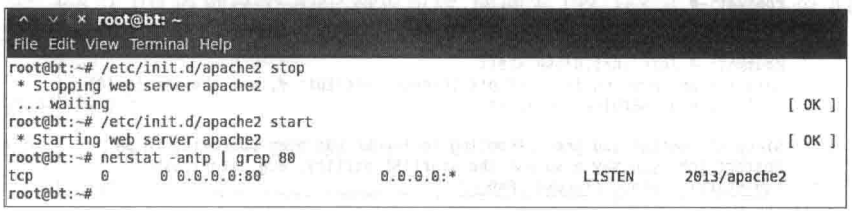

图 1-6　BT5 中 Apache 服务

2. MySQL 服务

如图 1-7 所示，通过命令启动 MySQL 服务器，然后登录到 MySQL，其中登录用户名是 root，密码是 toor。

```
root@bt:~# /etc/init.d/mysql start
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service mysql start

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the start(8) utility, e.g. start mysql
mysql start/running, process 2218
root@bt:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.1.63-0ubuntu0.10.04.1 (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

图 1-7　BT5 中 MySQL 服务

3. SSH 服务

SSH 服务可以应用在很多的场景下，比如 SSH tunneling、SCP 文件传输、远程登录等。要启用 BT5 的 SSH 服务，要在命令下依次输入 sshd-generate 和/etc/init. d/ssd start 命令，如图 1-8 所示。

```
root@bt: ~
File  Edit  View  Terminal  Help
+-----------------+
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
be:13:2b:d2:ce:76:2b:b2:97:bb:4e:97:5a:bb:22:70 root@bt
The key's randomart image is:
+--[ DSA 1024]----+
|                 |
|                 |
|                 |
|                 |
|        S        |
|  . E  ...       |
|   o ...=o       |
|    +oO++o       |
|    .XBB=+       |
+-----------------+
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# /etc/init.d/ssh start
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service ssh start

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the start(8) utility, e.g. start ssh
ssh start/running, process 1849
```

图 1-8　BT5 中 SSH 服务

1.2 网络数据包分析

本节通过一个实例介绍利用 Wireshark 分析网络数据包的方法。

网关的 IP 地址是 192.168.0.1，主机的 IP 地址是 192.168.0.104，当主机浏览网页 www.ccpc.edu.cn 后，数据包被捕获并且保存为 http.pcap。其中，网络拓扑和数据包的下载地址如图 1-9 所示。

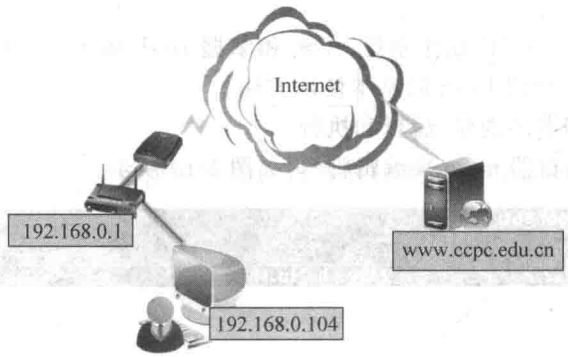

图 1-9　数据包下载地址：http://pan.baidu.com/share/link?shareid=367716&uk=4197835201

下面对捕获到的数据包进行详细的分析。

1. 数据包 No.2

DNS 请求包。既然主机 192.168.0.104 要浏览网页 www.ccpc.edu.cn，首先需要知道域名所对应的 IP 地址，所以主机向网关，同时也是本地的 DNS 服务器发送一个域名解析请求。本地 DNS 服务器于是向上一级的 DNS 服务器发送请求来解析域名。最终，www.ccpc.edu.cn 所对应的 IP 地址被解析成功，回传到 192.168.0.1。

2. 数据包 No.3

现在，网关 192.168.0.1 要把解析结果传给主机 192.168.0.104，但是，它还不知道 192.168.0.104 的 MAC 地址。于是 192.168.0.1 发送一个 ARP 广播包，询问 192.168.0.104 的 MAC 地址。

3. 数据包 No.4

主机 192.168.0.104 收到这个 ARP 请求包后，向网关 192.168.0.1 发送一个 ARP 回应包，把自己的 MAC 地址告诉网关。

4. 数据包 No.5

网关知道了 192.168.0.104 的 MAC 地址后，就把 DNS 回应包传送给它，这样主机 192.168.0.104 就知道了 www.ccpc.edu.cn 对应的 IP 地址是 210.47.128.15。

5. 数据包 No.6,No.7,No.8

主机通过 TCP 三次握手与 210.47.128.15 建立连接。

6. 数据包 No.9

主机向 210.47.128.15 发送 HTTP get 请求数据包。

1.3 Bash 脚本基础

BT5 是基于 UBUNTU 操作系统，了解和掌握 Bash 脚本，有助于更好地操作 BT5。本节将用几个实例来介绍 Bash 的基本使用方法。

实例 1：Bash 脚本的创建、编辑和执行。

(1) 使用文本编辑器 nano 来编辑脚本，如图 1-10 所示。

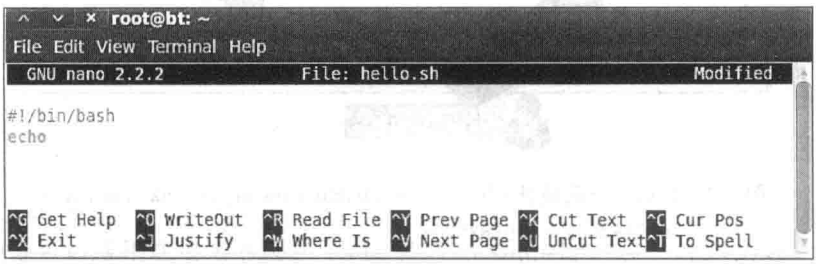

图 1-10 编辑 Bash 脚本

(2) 为脚本赋予可执行属性，如图 1-11 所示。

(3) 执行脚本，如图 1-12 所示。

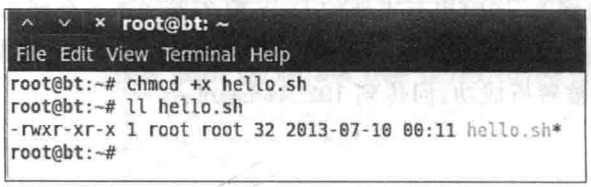

图 1-11 为脚本赋予可执行属性

图 1-12 命令行下执行脚本

实例 2：Bash 脚本中的全局变量和局部变量的使用方法。图 1-13 显示的是脚本的源代码，脚本的执行结果如图 1-14 所示。

```
#!/bin/bash
function localmessage
{
local message='hi, i am inside the function'
echo $message
}
message='hi, i am outside the function'
echo $message
localmessage
echo $message
```

图 1-13 variables.sh 源代码

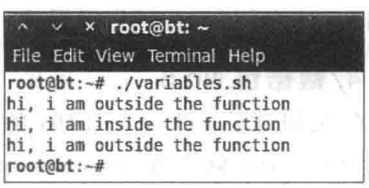

图 1-14 variables.sh 的执行结果

实例 3：Bash 脚本中的参数传递方法。图 1-15 显示的是脚本的源代码，脚本的执行结果如图 1-16 所示。

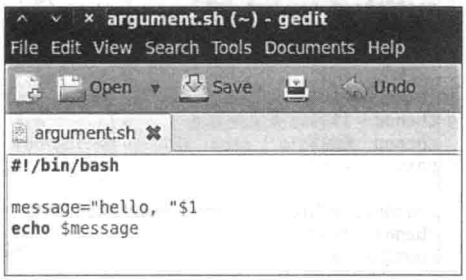

图 1-15　argument. sh 源代码

```
root@bt:~# ./argument.sh  ccpc
hello, ccpc
root@bt:~#
```

图 1-16　argument. sh 脚本的执行结果

实例 4：Bash 脚本中 if 语句使用方法。如图 1-17 所示是脚本的源代码，脚本的执行结果如图 1-18 所示。

```
#!/bin/bash
#
#

if [ $# != 1 ] ;then
   echo " Usage: $0  <IP> ";
   exit
fi

num=$(ping -c 1 $1 | grep "from" | wc -l)

if [ $num = 1 ]; then
   echo "$1 is up."
else
   echo "$1 is down."
fi
```

图 1-17　ping. sh 源代码

```
root@bt:~# ./ping.sh
 Usage: ./ping.sh  <IP>
root@bt:~# ./ping.sh  www.ccpc.edu.cn
www.ccpc.edu.cn is up.
root@bt:~#
```

图 1-18　ping. sh 执行结果

实例 5：Bash 脚本中 for 语句的使用方法。图 1-19 显示的是脚本的源代码，脚本的执行结果如图 1-20 所示。

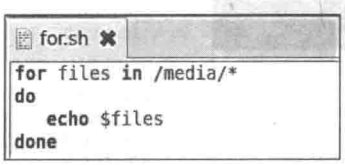

图 1-19　for. sh 脚本源代码

```
root@bt:~# chmod +x for.sh
root@bt:~# ./for.sh
/media/cdrom
/media/floppy
/media/floppy0
root@bt:~# ls /media/
cdrom  floppy  floppy0
root@bt:~#
root@bt:~#
```

图 1-20　for. sh 脚本执行结果

grep 命令的基本使用方法实例(实例 6～实例 11)如下。

实例 6：在文件中查找包含 chenou 字符串的行，如图 1-21 所示。

实例 7：在文件中查找包含 chenou 0602 字符串的行，如图 1-22 所示。

实例 8：在文件中查找包含 chenou 字符串的所有行，不区分字符的大小写，如图 1-23 所示。