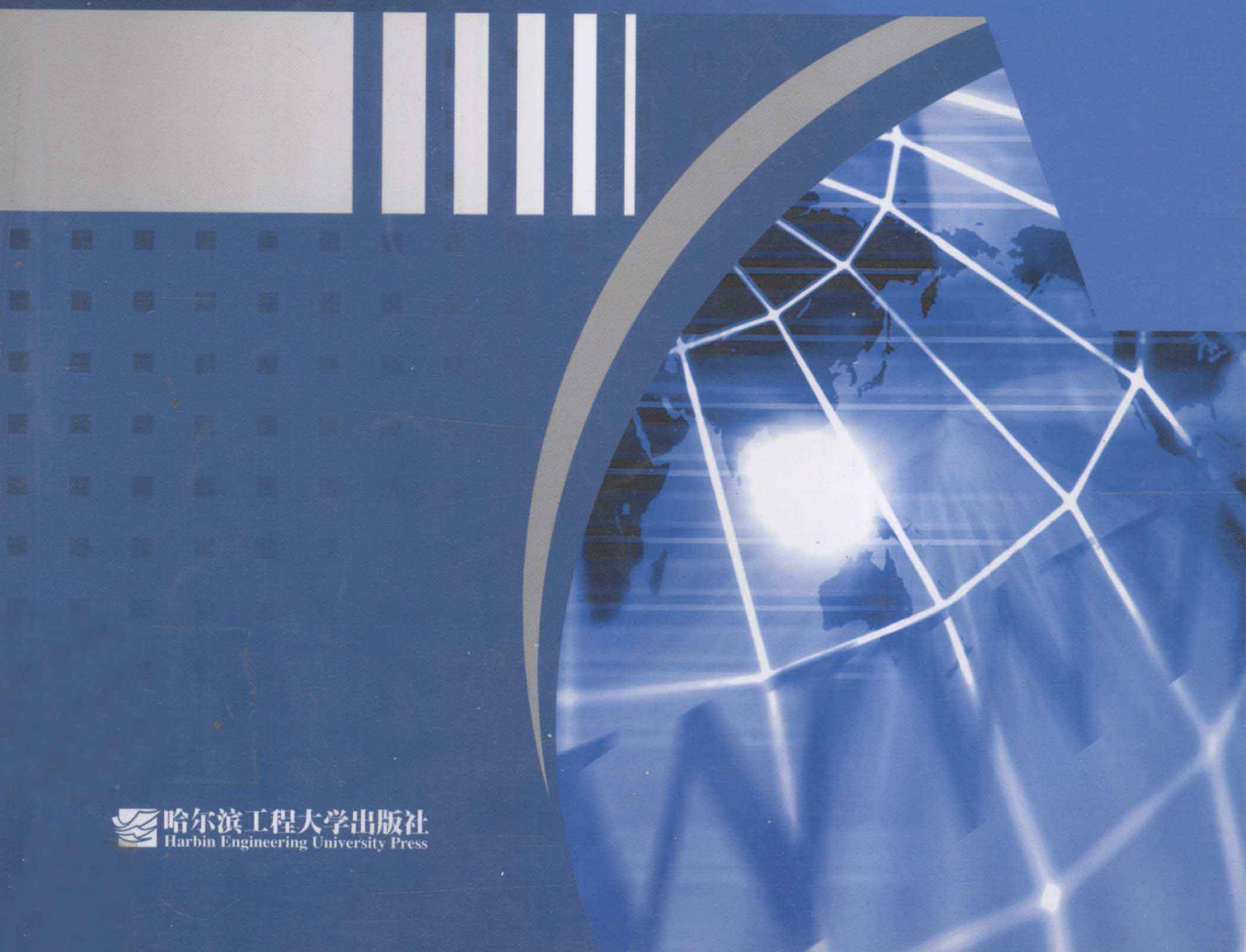
高职高专通用系列规划教材

GAOZHI GAOZHUAN TONGYONG XIELIE GUIHUA JIAOCAI

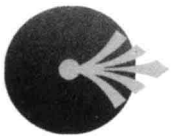
网络与信息安全实用教程

WANGLUO YU XINXI ANQUAN SHIYONG JIAOCHENG

主编 刘智涛



哈尔滨工程大学出版社
Harbin Engineering University Press



高职高专通用系列规划教材

GAOZHI GAOZHUAN TONGYONG XIELIE GUIHUA JIAOCAI

网络与信息安全实用教程

主　编　刘智涛

副主编　卢宏才　霍成义

参　编　武晶晶　程建峰

哈尔滨工程大学出版社

Harbin Engineering University Press

内容简介

本书主要介绍了网络与信息安全方面的部分重点、难点实验。全书共分四部分，主要内容包括基础安全、系统安全、网络安全、应用安全。通过本书的学习，读者能够对计算机网络与信息安全知识有一个比较系统的了解，掌握网络与信息安全中各种常用的实际操作与基本维护手段。

本书是为了适应高职院校以应用性为目的，以必需、够用为度，以岗位实用为准的教学特点而编写的一本适合高职院校学生培养的实用教材。书中的案例均已在真实环境或虚拟机环境下通过验证。本书适合高职院校电子商务、计算机网络和信息安全专业或相关相近专业的学生使用，也可作为从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员的参考书。

图书在版编目(CIP)数据

网络与信息安全实用教程/刘智涛主编. —哈尔滨:哈尔滨工程大学出版社,2009.9

ISBN 978-7-81133-545-3

Ⅰ.网… Ⅱ.刘… Ⅲ.计算机网络-安全技术-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2009)第 155127 号

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 哈尔滨工业大学印刷厂
开　　本 787mm×1 092mm　1/16
印　　张 11.25
字　　数 266 千字
版　　次 2009 年 9 月第 1 版
印　　次 2009 年 9 月第 1 次印刷
定　　价 21.50 元

http://press.hrbeu.edu.cn
E-mail:heupress@hrbeu.edu.cn

PREFACE 前言

随着信息技术和计算机网络的普及，网络和信息安全对社会生产生活的影响越来越大，网络提供了丰富的资源以便用户共享，提高了系统的灵活性和便捷性，但也正是因为这些特点，增加了网络的脆弱性，加大了网络受威胁和攻击的可能性。掌握必要的网络及信息安全操作技能是高职网络及信息安全专业学生必须具备的专业知识和技能之一。

本书共分四部分，分别是基础安全、系统安全、网络安全和应用安全。采用任务驱动模式，每个任务又以任务描述、相关知识、实现过程为主线，特别是实现过程中给出了详尽的操作步骤和具体的操作图解，基本涵盖了网络及信息安全实验中涉及的各个层次的主要知识。

本书以培养应用型和技能型人才为根本，以理论“实用、够用”为原则，注重实用性，通过提出问题、分析问题、解决问题这样一个认知过程，精心组织内容，力求重点突出，要点讲明，通俗易懂。本书针对高职高专教育特点，结合具体实验介绍了目前主流网络及信息安全管理、维护、操作等知识，有助于增强教学针对性、实用性。本书适合高等学校电子商务、计算机网络和信息安全专业或相近专业的学生使用，也可作为从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员的参考书。

本书由刘智涛担任主编，卢宏才、霍成义担任副主编，武晶晶、程建峰参编，全书由刘智涛统稿。在编写过程中参考了互联网上公布的一些相关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。其他参考文献在本书后列出。

由于作者水平有限，书中难免有疏漏和错误之处，希望读者批评指正，以期修订更新。

刘智涛

2009 年 5 月于天水

CONTENTS 目录

第一部分 基础安全

任务1 Caesar替代加密算法编程实现

【任务描述】

随着Internet及其相关技术的日益普及,电子商务已跨越局域网和广域网,加密各种敏感信息已经成为信息安全的至关重要的部分。信息安全又称为数据安全,早期的信息安全保护主要是借助于密码学(Cryptography)。作为保障数据安全的一种方式,数据加密起源于公元前2000年。埃及人是最先使用特别的象形文字作为信息编码的人。随着时间的推移,巴比伦、美索不达米亚和希腊文明都开始使用一些方法来保护他们的书面信息。

现代的计算机加密技术是为了网络安全应运而生的,它为我们进行一般的电子商务活动提供了安全保障,如在网络中进行文件传输、电子邮件往来和进行合同文本的签署等。在信息通信过程中要保证信息的完整性,可以使用密码技术实施数字签名、进行身份认证和对信息进行完整性校验,这些是当前实际可行的办法。为了保障信息系统和电子信息为授权者所用,可以利用密码进行系统登录管理,存取授权管理则是非常有效的办法,既保证了电子信息系统的可控性,同时也可以有效地利用密码和密钥来实施管理。

传统的加密方法有替代法、置换法。比较经典的是Caesar替代法以及由Caesar替代法改进后的Vigenere加密法。

通过本任务的实际操作与训练,要求学生掌握以下知识和技能:

(1)掌握利用编程实现算法的基本思想;

(2)加深对Caesar替代加密算法的理解;

(3)较熟练地使用程序开发软件Visual C++6.0。

【相关知识】

1.Caesar替代加密法

替代加密法是单字符加密法。称通信中所用的英文字母(共26个),数字(0~9),标点符号中每一个为明字符。将每个明字符用它们中的某一个代替,称为明字符的密字符。全体明字符的一一对应表称为密码表。

信息传输中,每个明字符用密字符去替代,明文块数据被密文块数据隐藏下来,只要通信双方保密这张密码表,通信过程中的安全性就有了保证。

先将英文26个字母a,b,c…依次排列,z后面接着排a,b,c…,它的加密方法就是把明文中所有字母都用它右边的第 k 个字母替代。这种映射关系表示为如下函数:

$$C = f(a) = (a + k) \bmod n$$

其中，a 表示明文字母；n 为字符集中字母的个数；k 为密钥。映射表示 $f(a)$ 等于 $(a+k)$ 除以 n 的余数。接受方接到密文后，再运用解密算法 $A=f(c)=(c-k)\bmod n$，还原为原来的明文，其中 A 表示明文，c 表示密文，k 表示密钥。

设 $k=3$（注：若取 $k=3$，则此密码体制通常叫做凯撒密码，因为它首先为儒勒·凯撒所使用），对于明文 P = gameisover，则有

$$f(\mathrm{g})=(7+3)\bmod 26=10=\mathrm{j}$$
$$f(\mathrm{a})=(1+3)\bmod 26=4=\mathrm{d}$$
$$f(\mathrm{m})=(13+3)\bmod 26=16=\mathrm{p}$$
$$\vdots \qquad\qquad \vdots$$

所以，密文 $C=Ek(\mathrm{P})=$ jdphlvryhu，当接受方接受到密文后，结合密钥，运用解密算法还原得到明文为 gameisover。

2. Vigenere 加密法

对于 Caesar 替代法，容易受到攻击者的频率攻击。攻击者在截获密文后，分析密文各个字母出现的频率，便可以猜想出各个字母的对应关系。基于这个缺陷，法国人 Vigenere 改进了 Caesar 算法，提出了 Vigenere 替代算法。

Vigenere 替代算法是循环使用有限个字母来实现替代的一种方法。若明文信息 $M_1M_2M_3\cdots M_n$，采用 n 个字母（n 个字母为 $B_1B_2B_3\cdots B_n$）替代法，那么，M_n 将根据字母 B_n 的特征来替代，M_{n+1} 又将根据 B_1 的特征来替代……，如此循环，可见 $B_1, B_2, B_3, \cdots, B_n$ 就是加密的密钥。

这种加密的加密表是以字母表移位为基础把 26 个英文字母进行循环移位，排列在一起，形成 26×26 的方阵。该方阵被称为维吉尼亚表，采用的算法为

$$C_i=(aM_i+B_i)\bmod n \qquad (i=1,2,3,\cdots,n)$$

当接受方接受到密文后，通过解密算法 $M_i=(1/a)(\bmod n)(C_i-B_i)(\bmod n)$ 还原出明文。

下面编程具体实现 Caesar 替代加密算法。

【实现过程】

下面的程序编写及调试均可在 VC6.0 中完成，输入的明文（Plaintext）和结果密文（Ciphertext）均以英文大写字母的形式出现，输入时以"\0"作为结束输入标志，程序源代码如下：

```
#include<stdio.h>
#include<string.h>
main()
{
  char str1[100];
  char str2[100];
  int i;
  char ch;
  printf("Please input plaintext:");
  gets(str1);
  for(i=0;(ch=str1[i])!='\0';i++)
```

```
    }
    if(ch == 'X')
      str2[i] = 'A';
    else if(ch == 'Y')
      str2[i] = 'B';
    else if(ch == 'Z')
      str2[i] = 'C';
    else str2[i] = str1[i] + 3;
    }
  printf(" \ nThe ciphertext is: %s \ n",str2);
}
```

1.在 VC6.0 中输入源程序,如图 1-1 所示。

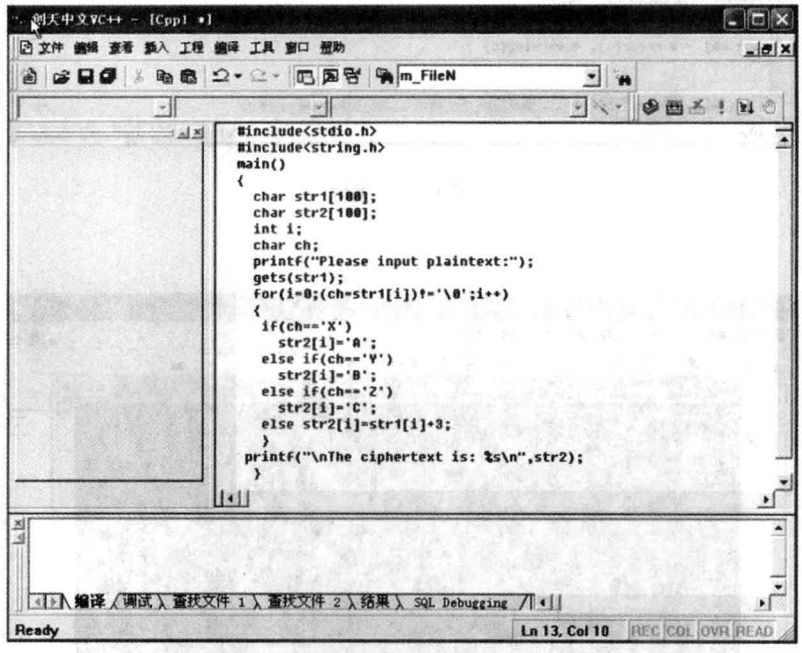


图 1-1 源程序

2.调试:执行“编译”菜单下的“编译”命令,如图 1-2 所示。

3.执行 Cpp1.exe 后,当我们输入 GAMEISOVER 时,输出结果是 JDPHLVRYHU,如图 1-3 所示。

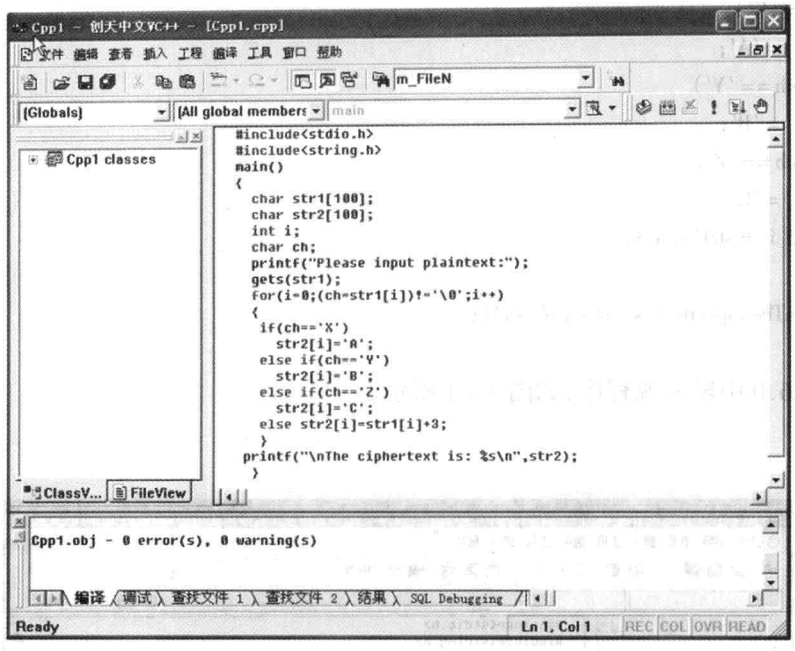

Cpp1 - 创天中文VC++ - [Cpp1.cpp]
文件 编辑 查看 插入 工程 编译 工具 窗口 帮助
m_FileN
(Globals)
(All global members
main
Cpp1 classes
ClassV...
FileView
#include<stdio.h>
#include<string.h>
main()
{
char str1[100];
char str2[100];
int i;
char ch;
printf("Please input plaintext:");
gets(str1);
for(i=0;(ch=str1[i])!='\0';i++)
{
if(ch=='X')
str2[i]='A';
else if(ch=='Y')
str2[i]='B';
else if(ch=='Z')
str2[i]='C';
else str2[i]=str1[i]+3;
}
printf("\nThe ciphertext is: %s\n",str2);
}
Cpp1.obj - 0 error(s), 0 warning(s)
编译 调试 查找文件 1 查找文件 2 结果 SQL Debugging
Ready
Ln 1, Col 1
REC COL OVR READ

图 1-2 编译

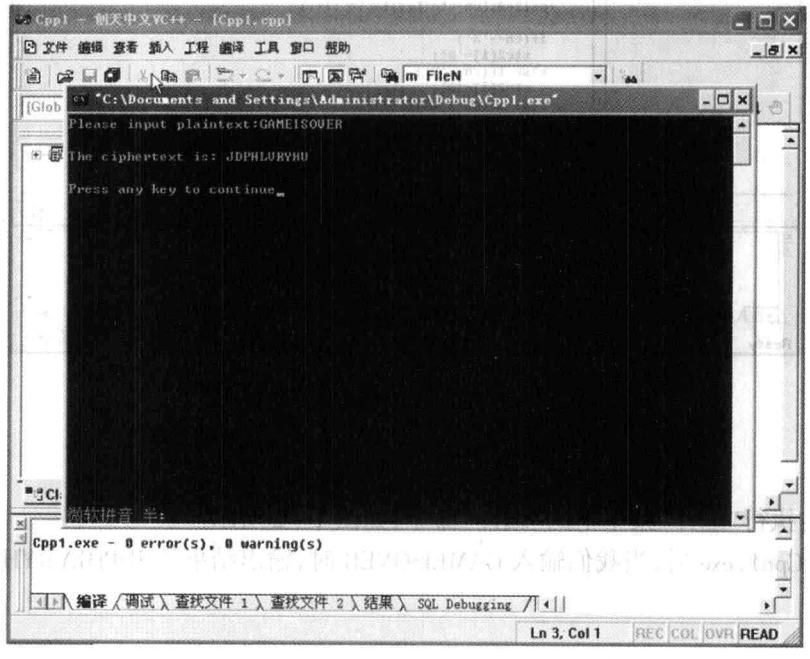

Cpp1 - 创天中文VC++ - [Cpp1.cpp]
文件 编辑 查看 插入 工程 编译 工具 窗口 帮助
m_FileN
"C:\Documents and Settings\Administrator\Debug\Cpp1.exe"
Please input plaintext:GAMEISOVER
The ciphertext is: JDPHLVRYHU
Press any key to continue
Cpp1.exe - 0 error(s), 0 warning(s)
编译 调试 查找文件 1 查找文件 2 结果 SQL Debugging
Ln 3, Col 1
REC COL OVR READ

图 1-3 结果

任务 2　常用网络管理命令的使用

【任务描述】

本实验详细给出以下几个 Windows 系统自带的网络方面的命令，只有熟练使用它们才会给信息收集和安全防御带来极大的便利。

通过本任务的实际操作与训练，要求学生掌握以下知识和技能：

(1)掌握各种主要命令的作用；

(2)掌握各种网络命令的主要测试方法；

(3)理解各种网络命令主要参数的含义。

【相关知识】

在网络调试的过程中，常常要检测服务器和客户机之间是否连接成功、希望检查本地计算机和某个远程计算机之间的路径、检查 TCP/IP 的统计情况以及系统使用 DHCP 分配 IP 地址时掌握当前所有的 TCP/IP 网络配置情况，以便及时了解整个网络的运行情况，确保网络的连通性，保证整个网络的正常运行。在 Windows Server 2003 中提供了以下命令行程序。

(1)ping　用于测试计算机之间的连接，这也是网络配置中最常用的命令；

(2)ipconfig　用于查看当前计算机的 TCP/IP 配置；

(3)netstat　显示连接统计；

(4)tracert　进行源主机与目的主机之间的路由连接分析；

(5)arp　实现 IP 地址到物理地址的单向映射。

为了使任务成功进行，需要有以下实验设备：

(1)安装有 Windows 2003 Server 操作系统的计算机；

(2)至少有两台计算机通过交叉双绞线相连或通过集线器相连。

【实现过程】

1. ping 命令

ping 用于确定网络的连通性。命令格式为

ping 主机名/域名/IP 地址

一般情况下，用户可以通过使用一系列 ping 命令来查找问题出现在什么地方，或检验网络运行的情况。典型的检测次序及对应的可能故障如下。

(1)ping 127.0.0.1　如果测试成功，表明网卡、TCP/IP 协议的安装、IP 地址、子网掩码的设置正常。如果测试不成功，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

(2)ping 本机 IP　如果测试不成功，则表示本地配置或安装存在问题，应当对网络设备和通信介质进行测试、检查并排除。

(3)ping 局域网内其他 IP　如果测试成功，表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码不正确或网卡配置错误或电缆系统有问题。

(4)ping 网关 IP　这个命令如果应答正确,表示局域网中的网关或路由器正在运行并能够作出应答。

(5)ping 远程 IP　如果收到正确应答,表示成功地使用了缺省网关。对于拨号上网用户则表示能够成功地访问 Internet。

(6)ping localhost　localhost 是系统的网络保留名,它是 127.0.0.1 的别名,每台计算机都应该能够将该名字转换成该地址。如果没有做到这点,则表示主机文件(/Windows/host)存在问题。

(7)ping www.163.com(一个著名网站域名)　对此域名执行 ping 命令,计算机必须先将域名转换成 IP 地址,通常是通过 DNS 服务器。如果这里出现故障,则表示本机 DNS 服务器的 IP 地址配置不正确,或 DNS 服务器有故障。

如果上面所列出的所有 ping 命令都能正常运行,那么计算机进行本地和远程通信基本上就没有问题了。但是,这些命令的成功并不表示所有的网络配置都没有问题,例如,某些子网掩码错误就可能无法用这些方法检测到。ping 命令的常用参数选项如下。

ping IP - t　连续对 IP 地址执行 ping 命令,直到被用户以 Ctrl + C 中断。

ping IP - l 2000　指定 ping 命令中的数据长度为 2000 字节,而不是缺省的 32 字节。

ping IP - n　执行特定次数的 ping 命令。

ping IP - f　强行不让数据包分片。

ping IP - a　将 IP 地址解析为主机名。

2.IP 配置程序命令 ipconfig

发现和解决 TCP/IP 网络问题时,先检查出现问题的计算机的 TCP/IP 配置。可以使用 ipconfig 命令获得主机 TCP/IP 配置信息,包括 IP 地址、子网掩码和默认网关。命令格式为

ipconfig/options

其中 options 选项信息如下。

/?　显示帮助信息。

/all　显示全部配置信息。

/release　释放指定网络适配器的 IP 地址。

/renew　刷新指定网络适配器的 IP 地址。

/flushdns　清除 DNS 解析缓存。

/registerdns　刷新所有 DHCP 租用和重新注册 DNS 名称。

/displaydns　显示 DNS 解析缓存内容。

使用带/all 选项的 ipconfig 命令时,将给出所有接口的详细配置报告,包括任何已配置的串行端口。使用 ipconfig/all 可以将命令输出重定向到某个文件,并将输出粘贴到其他文档中,也可以用该输出确认网络上每台计算机的 TCP/IP 配置,或者进一步调查 TCP/IP 网络问题。例如,若计算机配置的 IP 地址与现有的 IP 地址重复,则子网掩码显示为 0.0.0.0。图 1 - 4是使用 ipconfig/all 命令输出,显示了当前计算机配置的 IP 地址、子网掩码、默认网关以及 DNS 服务器地址等相关的 TCP/IP 信息。

3.显示网络连接程序 netstat

netstat 命令的功能是显示网络连接、路由表和网络接口信息,可以让用户得知目前都有哪些网络连接正在运作,其命令格式为

netstat [- a] [- e] [- n] [- s] [- p protocol] [- r] [interval]

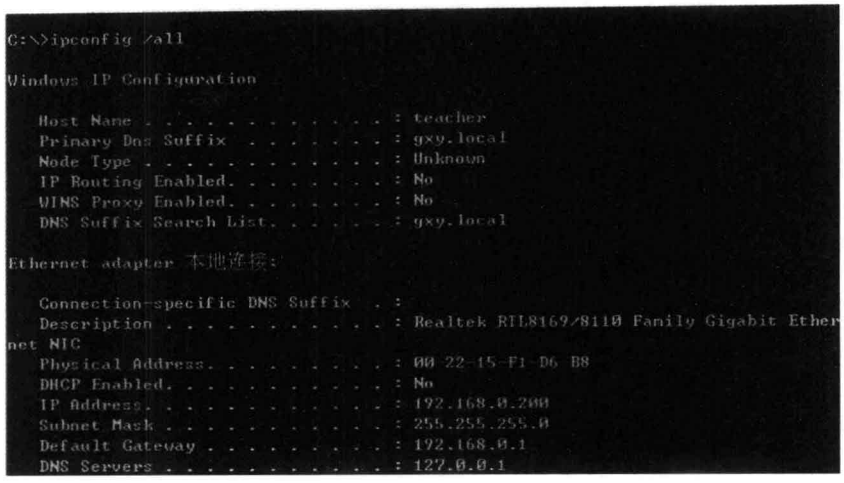


图 1-4 使用 ipconfig/all 命令查看 TCP/IP 配置

参数说明如下。

(1)netstat -s -s 选项能够按照各个协议分别显示其统计数据。这样就可以看到当前计算机在网络上存在哪些连接,以及数据包发送和接收的详细情况等。如果应用程序(如 Web 浏览器)运行速度比较慢,或者不能显示 Web 页之类的数据,那么可以用本选项来查看一下所显示的信息。仔细查看统计数据的各行,找到出错的关键字,进而确定问题所在。

(2)netstat -e -e 选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量,也有接收的数据报数量。使用这个选项可以统计一些基本的网络流量。

(3)netstat -r -r 选项可以显示关于路由表的信息,类似后面所讲使用 route print 命令时看到的信息。除了显示有效路由外,还显示当前有效的连接。

(4)netstat -a -a 选项显示一个所有的有效连接信息列表,包括已建立的连接(ESTABLISHED),也包括监听连接请求(LISTENING)的那些连接。

(5)netstat -n 显示所有已建立的有效连接,以数字格式显示地址和端口号。

(6)netstat -p protocol 显示由 protocol 指定的协议的连接。protocol 可以是 TCP 或 UDP。如果与 -s 选项并用显示每个协议的统计,protocol 可以是 TCP,UDP,ICMP 或 IP。

(7)netstat interval 重新显示所选的统计,在每次显示之间暂停 interval 秒。按 Ctrl + B 键停止,重新显示统计。如果省略该参数,netstat 将打印一次当前的配置信息。

当前最为常见的木马通常是基于 TCP/UDP 协议进行 Client 端与 Server 端之间的通信,既然利用到这两个协议,就不可避免要在 Server 端(就是被种了木马的机器)打开监听端口来等待连接。例如冰河使用的监听端口是 7626,Back Orifice 2000 则是使用 54320 等。我们可以利用 netstat 命令查看本机开放端口的方法来检查自己是否被种了木马或其他黑客程序。进入到命令行下,使用 netstat 命令的 a 和 n 两个参数的组合,如图 1-5 所示。

其中,Active Connections 是指当前本机的活动连接;Proto 是指连接使用的协议名称;Local Address 是本地计算机的 IP 地址和连接正在使用的端口号;Foreign Address 是连接该端口的远程计算机的 IP 地址和端口号;State 则是表明 TCP 连接的状态,可以看到后面几行的

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1050           0.0.0.0:0              LISTENING
```

图 1-5 使用 netstat 命令显示网络连接

监听端口是UDP协议的,所以没有 State 表示的状态。

4.路由分析诊断程序 tracert

这个应用程序主要用来显示数据包到达目的主机所经过的路径。通过执行一个 tracert 到对方主机的命令之后,结果返回数据包到达目的主机前所经历的路径详细信息,并显示到达每个路径所消耗的时间。

这个命令同 ping 命令类似,但它所看到的信息要比 ping 命令详细得多,它能反馈显示送出的到某一站点的请求数据包所走的全部路由,以及通过该路由的 IP 地址,通过该 IP 的时间是多少。Tracert 命令还可以用来查看网络在连接站点时经过的步骤或采取哪种路线,如果是网络出现故障,就可以通过这条命令来查看是在哪儿出现问题的。例如可以运行 tracert www.163.com 就将看到网络在经过几个连接之后所到达的目的地,也就知道网络连接所经历的过程。

路由分析诊断程序 tracert 通过向目的地发送具有不同生存时间的 ICMP 回应报文,以确定至目的地的路由。也就是说,tracert 命令可以用来跟踪一个报文从一台计算机到另一台计算机所走的路径。命令格式为

tracert [-d] [-h maximum _ hops] [-j host-list] [-w timeout] target _ name

参数说明如下。

-d 不进行主机名称的解析。

-h maximum _ hops 最大的到达目标的跃点数。

-j host-list 根据主机列表释放源路由。

-w timeout 设置每次回复所等待的毫秒数。

比如用户在上网时,想知道从自己的计算机如何连接到网易主页,可在 MS-DOS 方式下输入命令 tracert www.163.com,如图 1-6 所示。

最左边的数字称为“hops”,是该路由经过的计算机数目和顺序。“10 ms”是向经过的第一个计算机发送报文的往返时间,单位为 ms。由于每个报文每次往返时间不一样,tracert 将显示三次往返时间。如果往返时间以“*”显示,而且不断出现“Request timed out”的提示信息,则表示往返时间太长,此时可按下 Ctrl + C 键离开。要是看到四次“Request timed out”信息,则极有可能遇到拒绝 tracert 询问的路由器。在时间信息之后,是计算机的名称信息,通

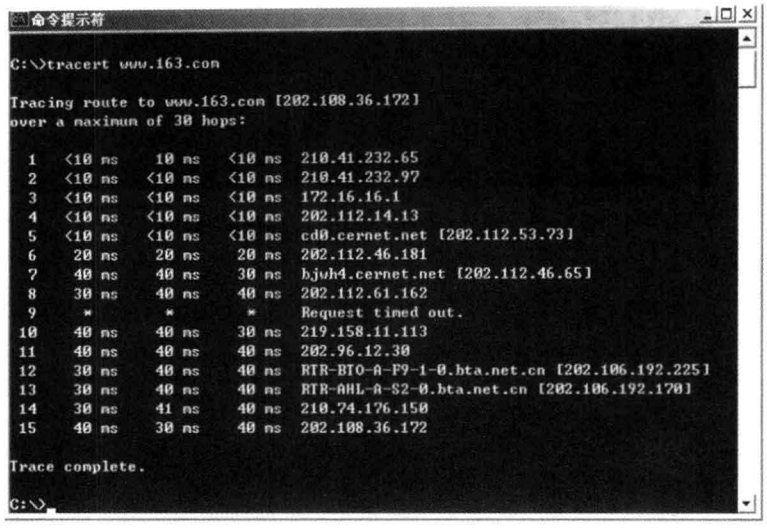


图 1-6 tracert 命令的运用

常是便于人们阅读的域名格式,也有IP地址格式。它可以让用户知道自己的计算机与目的计算机在网络上距离有多远,要经过几步才能到达。

tracert 最多会显示 30 段“hops”,上面会同时指出每次停留的响应时间,以及网站名称和沿路停留的 IP 地址。一般来说,连接上网速度是由连接到主机服务器的整个路径上所有相应事物的反应时间总和决定的,这就是为什么一个经过 5 段跳接的路由器 hops,如果需要1 s 来响应的话,会比经过 9 段跳接但只需耀 200 ms 响应的路由器 hops 来得糟糕。通过 tracert 所提供的资料,可以精确指出到底连接哪一个服务器比较划算。但是,tracert 是一个运行得比较慢的命令(如果用户指定的目标地址比较远),每个路由器用户大约需要给它 15 s 来发送报文和接收报文。

5. ARP 地址解析协议

ARP 是 TCP/IP 协议族中的一个重要协议,用于把 IP 地址映射成对应网卡的物理地址。使用 ARP 命令,能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。

使用 ARP 命令可以人工方式设置静态的网卡物理/IP 地址对,使用这种方式可以为缺省网关和本地服务器等常用主机进行本地静态配置,这有助于减少网络上的信息量。

按照缺省设置,ARP 高速缓存中的项目是动态的,每当发送一个指定地点的数据报并且此时高速缓存中不存在当前项目时,ARP 便会自动添加该项目。

常用命令选项如下。

(1)arp -a 用于查看高速缓存中的所有项目。

(2)arp -a IP 如果有多个网卡,那么使用 arp -a 加上接口的 IP 地址,就可以只显示与该接口相关的 ARP 缓存项目。

(3)arp -s IP 物理地址 向 ARP 高速缓存中人工输入一个静态项目。该项在计算机引导过程中将保持有效状态,或者在出现错误时,人工配置的物理地址将自动更新该项目。

(4)arp -d IP 使用本命令能够人工删除一个静态项目。

图 1-7 是带参数的 ARP 命令的简单实现。

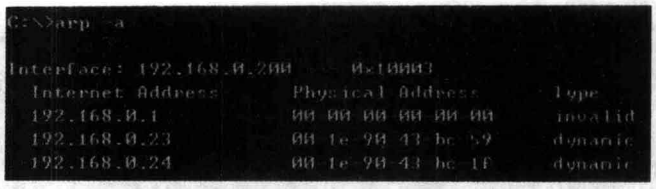


图 1-7 arp 命令中 -a 和 -s 参数的运用

任务3　加密工具PGP软件的使用

【任务描述】

PGP加密软件是美国Network Associate Inc生产的免费软件，可用它对文件、邮件进行加密，在常用的Winzip，Word，Arj，Excel等软件的加密功能均告可被破解时，选择PGP对自己的私人文件、邮件进行加密不失为一个好办法。除此之外，还可与同样装有PGP软件的朋友互相传递加密文件，非常安全可靠。

通过本任务的实际操作与训练，要求学生掌握以下知识和技能：

(1)PGP的下载及安装；

(2)使用PGP产生和管理密钥；

(3)使用PGP进行加密/脱密、签名/验证；

(4)使用PGP销毁秘密文件。

【相关知识】

PGP软件的英文全名是Pretty Good Privacy，它广泛用于电子邮件和其他场合，是一个十分出色的加密软件。

PGP最早的版本是由美国的Philip Zimmermann在1991年夏天发布的。Philip Zimmermann将PGP免费地张贴出去。由于PGP的优良特性及其开放性，PGP和Linux并列为最伟大的自由软件。1992年2月，PGP的新版本在欧洲发布了。PGP的国际版本在美国境外开发，打破了美国政府的软件出口限制，PGP的国际版本带有i的后缀，如PGP6.5.1i。2002年12月3日的最新版本PGP8.0可以从挪威的www.pgpi.com下载。PGP把整套加密技术交给用户，它没有采用密钥公证制度，也是出于避免国家介入个人隐私的考虑。

PGP自发布以来，赢得了全球的亿万用户的支持，已经成为电子邮件加密事实上的标准。PPG的功能强大，包括所有的源程序代码，还提供各种语言函数接口的免费加密函数工具包，让没有高深密码学知识的程序员也能够很容易地在应用程序中添加加密和安全认证的功能，可以极大地降低在应用程序中关于加密和认证模块的开发成本。

PGP实现了大部分的加密和认证的算法，如Blowfish，CAST，DES，TripleDES，IDEA，RC2，RC4，RC5，Safer，Safer-SK等传统的加密方法，以及MD2，MD4，MD5，RIPEMD－160，SHA等散列算法，当然也包括D－H，DSA，Elgamal，RSA等公开密钥加密算法。PGP先进的加密技术使它成为最好的、攻击成本最高的安全性程序。

PGP的巧妙之处在于它汇集了各种加密方法的精华。PGP兼有加密和签名两种功能。数据的加密主要使用速度快，安全性能好的IDEA算法。对IDEA的密钥进行加密使用RSA算法，因为它是目前最好的公钥系统，这样，把两种加密体制巧妙地结合起来，可扬长避短，各尽其能。PGP用MD5作为散列函数，保护数据的完整性，同时和加密算法相结合，提供了签名功能。PGP的加密功能和签名功能可以单独使用，也可以同时使用，由用户自行决定。

PGP的密钥管理体制是独具特色的。为了摆脱国家的控制，PGP不设立密钥公证机制，

它使用的是一种类似于日常社交生活中的介绍机制。你的公钥通过你的朋友介绍给你的新朋友,你的新朋友基于对介绍人的信任而给你的公钥以一定程度的信任。你的朋友在作介绍时使用了他自己的数字签名,这种介绍的方式符合人们的生活习惯,亲切而自然。当然如果介绍人信誉不高或者不负责任,那么信任度就会打折扣。

从密码体制上来说,PGP 使用了现代加密技术,其安全性应当是有保证的。但从密钥的安全性来说,PGP 使用了一个用户随机产生的 RSA 密钥和打开这个密钥的口令,保护好自己的口令是一件关键性的事情。公钥的篡改和冒充是 PGP 的主要威胁。另外,PGP 的源代码是公开的,有可能受到攻击,所以一定要从可靠的站点上下载可靠的程序。如果不小心把黑客假冒的 PGP 程序安装到你的机器上,那后果将不堪设想。

【实现过程】

1. PGP 的下载及安装

PGP 是免费的软件,可以自由下载。在挪威的 www.pgpi.com 网站中可以下载到最新的版本。压缩后的容量大约有 8 MB。打开国际 PGP 站点主页后,可直接选择下载最新版本,在下载时要选择的应用平台是 Windows。下载过程十分简单,用户可自行完成。下载完毕后准备安装。

找到刚下载的 PGP 自解压文件,双击文件名开始安装。首先进入欢迎界面,如图 1-8 所示。

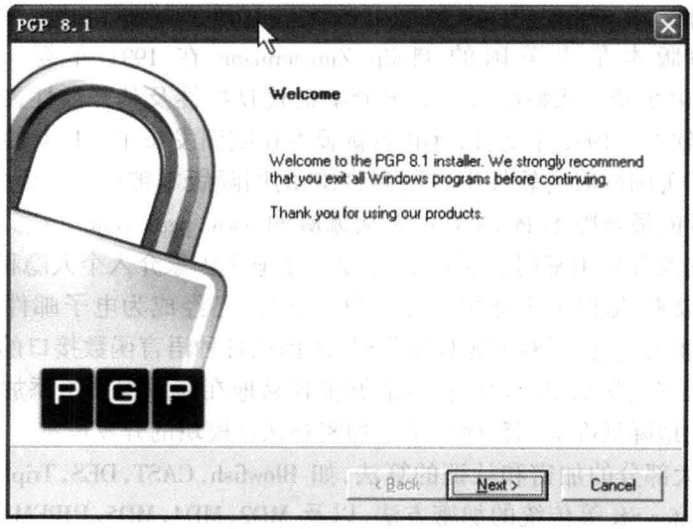


图 1-8 PGP 软件安装欢迎界面

单击“Next >”按钮,阅读许可协议后单击“Yes”按钮,如图 1-9 所示,阅读 Read Me 后单击“Next >”按钮,如图 1-10 所示。