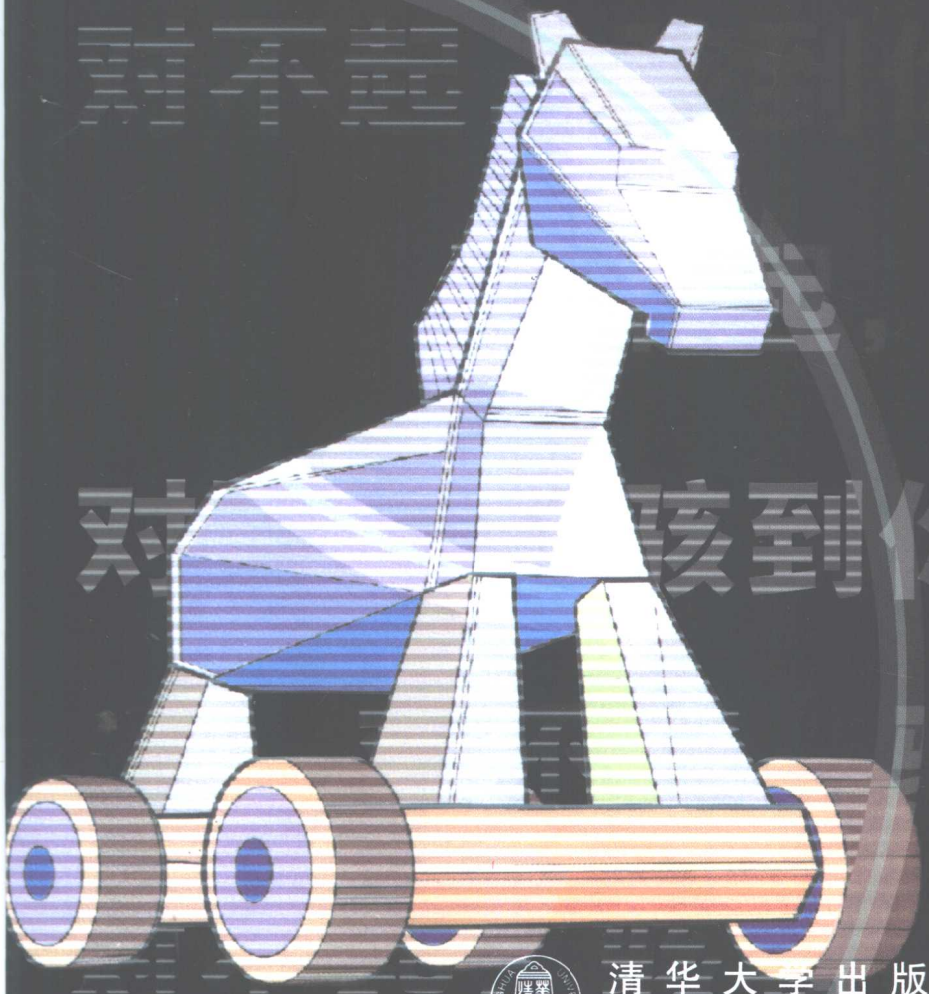
黑客攻防对策之

木马篇

秘密客　编著



清华大学出版社
http://www.tup.tsinghua.edu.cn

黑客攻防对策之木马篇

秘密客　编著

清 华 大 学 出 版 社

(京)新登字 158 号

北京市版权局著作权合同登记号：01-2001-4395 号

内 容 简 介

黑客技术是一把双面利刃。我们了解黑客的目的不是为了入侵他人主机，而在于懂得怎样防护自己的系统，以及保护自己的文件数据不受他人攻击。

本书是《黑客攻防对策》的姐妹篇，是一本详细介绍木马检测与清除技术的中级参考用书。本书结合网络安全与操作系统的种种漏洞，提出一些有效地填补漏洞的方法，进而衍生出 TCP/IP、防火墙等实际问题，带你进入黑客攻防的实际问题中，让你更好地掌握防御及抵抗其进攻的对策。

本书语言浅显易懂、内容丰富，结合实际案例进行分析说明，实用性强，是网络管理员和网络工程师的最佳参考用书，同时也适用于广大的电脑网络爱好者。

书　　名：黑客攻防对策之木马篇
作　　者：秘密客　编著
出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑：陈仕云
印 刷 者：北京通州大中印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　**印张**：14.75　**字数**：338 千字
版　　次：2002 年 5 月第 1 版　2002 年 5 月第 1 次印刷
书　　号：ISBN 7-900641-46-7
印　　数：0001～6000
定　　价：29.00 元(附光盘)

序

当年特洛伊战争（Trojan War），希腊军队久久无法攻陷特洛伊（Troy）城，于是便使计制作一匹大木马，在其中暗藏士兵，之后大军留下木马佯装撤退，特洛伊人不明事由，将大木马拖入城内，并设宴庆祝，待夜幕降临之际，士兵出了木马，与折回的希腊大军来个里应外合、攻占该城，从此有了特洛伊木马（Trojan horse）的典故。

网络上的每台计算机，就像是身陷于特洛伊战争中的特洛伊城，而希腊士兵则化身成为网络黑客，搭乘已经有了各种美丽化身的“木马”，一一攻陷每一座特洛伊城。

伴随木马入侵所延伸的问题，首当其冲的就是“网络安全”，难道计算机真的就这么毫无防范吗？这个问题一直是每个 MIS 人员的梦魇，因为即使是再安全的防火墙，也无法保证它没有漏洞。尤其随着微软每一代 Windows 的上市，相关的漏洞消息就会被翻出来炒作，这些漏洞顺理成章地演变成黑客入侵的通道。

漏洞无时无刻地被发现，而入侵主机的方式也有千百种，本书将从这些入口逐一渗透，除了提供宝贵的实际经验之外，也将审视 Windows 9x/ME/NT/2000 等系统的安全漏洞，并提供实际的入侵案例，进而衍生出 TCP/IP、防火墙等相关问题的概念，让您能够使其招以能防其道。

“黑人者，人恒黑之”，本书虽然提供实际的黑客案例，但其主要目的绝非教导读者破坏他人计算机、窃取别人隐私，而是要让其认识到网络安全上的疏忽，进而提出相关的防范措施。毕竟知己知彼，了解敌人多一分，也就多一分安全。

最后再提醒您一次，任意侵入他人系统、窃取文件的行为都是违法的，切勿使用该技巧来胡作非为。若是幸运地入侵他人计算机，也要在心中抱着歉意，默念一句……

“对不起，骇到你！”

作者　秘密客

本书姐妹篇

黑客攻防对策

秘密客　编著

定价：34.00 元（附光盘）

本书是一本了解黑客入侵手段，从而掌握各种防护对策的最佳入门手册。通过介绍黑客可能采取的进攻手段——电子邮件、网络网页、工具程序、木马程序等，详细分析了黑客进攻的方法和防范对策，从而对黑客攻击有一个充分的认识。

全书以实际的案例形式，带您走进黑客的世界，在了解黑客进攻手法的基础上，学习掌握常用的防御对策，使得黑客无从下手，无所遁形，让您安全地畅游在 internet 网络世界。

本书是信息安全从业人员和网络管理员的最佳助手，同时适用于广大的网络爱好者。

目　录

第 1 章　黑客骑着木马光临

网络消息:

全球病毒监测网发现一种新的病毒？Qaz.A.特洛伊木马。这种病毒通过联网的驱动器进行传播，并在 Windows 9x 和 Windows NT 系统下运行。

一旦 Qaz.A.特洛伊被启动，它将产生一个登录的字符串，并指向一个蠕虫文件，每次系统重启时，该病毒都将被再次运行。Qaz.A.特洛伊通过打开 7597Port 去接听远程命令，它也像后门（Backdoor）特洛伊一样是秘密进行的。蠕虫会周期性地搜索网络上的 Notepad.exe 文件，一旦找到，会将原始的 Notepad.exe 改名为 Notepad.com，并将蠕虫文件的副本作为 Notepad.exe 驻留在系统中。一旦 Notepad.exe 被客户端的机器运行，感染的循环将持续扩大。

1-1　木马与病毒

荷马史诗中描述一位名为 Hellen 的希腊皇后被特洛伊王国的王子所骗，于是希腊国王派兵攻打特洛伊城，此番战争打了十年，却始终无法攻陷特洛伊城，于是便想了一条计策，制作一匹大木马，里面藏满了全副武装的士兵，留下木马后佯装撤退，特洛伊人果然上当，以为希腊人已放弃攻打城墙，便将木马拖入城内，并设宴庆祝。等到夜晚来临，特洛伊城的士兵喝得大醉毫无戒心，而木马内的士兵一举而出，与早已埋伏在附近的希腊士兵里应外合，攻下了特洛伊城。此即著名的特洛伊战争，也就是木马屠城记，亦为特洛伊木马（Trojan horse）的典故。

网络上常有些让你免费下载的小程序，“查看你的密码是否被猜出”、“测试你的计算机性能”，或是可爱的卡通人物，只要你下载运行后，它便会在你的计算机中打开一个后门任人进出。大部分的木马程序是由用户自己带入计算机系统的，就像特洛伊人打开城门让木马进来一样。

在网络的世界模式中是由一台主机提供服务，也就是服务器（Server），另一台主机接受服务，即客户端（Client），作为服务端的主机会打开一个 Port 进行监听的动作（Listen），当客户端服务器提出连接要求时，服务器上相对应的程序便会自动运行，答应客户端的请求。举例来说，运行 Telnet 便是利用 Port 23，运行 FTP 是用 Port 21，浏览网页时即打开 Port 80。所以特洛伊木马通常会有两个程序，一个是给别人运行用的“服务器端”程序，一个是黑客自己使用的“客户端程序”。当上当的用户运行“服务器端”程序后，黑客即可用手边的“客户端程序”将对方的电脑加以控制、对数据进行存取等。

几个较常见的木马程序如 Back Orifice、Net Bus，就是用远程控制程序让你可在自己的

计算机远程控制对方的主机，执行你所下达的命令。

1-1-1 木马不是病毒

一般杀毒软件会将木马程序视为病毒，如根据趋势科技的定义："特洛伊木马型病毒是一种具有运行非预期或未授权（恶意）之功能的程序，例如显示信息、删除文件或将磁盘格式化。特洛伊木马型病毒不会感染其他寄宿文件，因此不需要进行清除。清除特洛伊木马型病毒的方法是直接删除受感染的程序"。

虽然称为病毒，但木马程序实际上和病毒仍然有不同的地方，最大的差别在于木马程序没有复制能力，而病毒会复制、传染，且要有宿主才能生存以进行破坏，特洛伊木马却能够自己独立运行破坏功能，也就是说当计算机中了病毒后，很快整个系统都会遍布病毒的同类，而木马程序始终就是那一个。

特洛伊木马通常都会伪装成有用的程序，通过和其他应用程序相结合，或是和图片、声音结合，隐蔽木马的真面目，诱惑用户在没有戒心的情况下运行，而病毒却不用，因此木马程序会比病毒大许多。所以当你收到了别人发送的有趣小程序（如会在屏幕上走动翻滚的 Hello Ketty、酷企鹅），甚至是图文件、声音文件，其中都可能隐藏了木马程序，在你欣赏图片听音乐的同时，也已经将后门打开。

木马程序虽不像病毒会扩散、有感染力，但其破坏能力绝对不低于病毒。以下为特洛伊木马的特征：

（1）让用户无法运行任何功能。

（2）程序的体积不大，运行时并不会占系统太多资源，让用户不会感到异样。

（3）一经运行后就会自动登录在启动区，之后每次打开 Windows 便会自动加载。

（4）不需要允许即可获得计算机的使用权。

（5）会自动变更文件名或隐藏。

1-1-2 木马的功能与作用

不管此前你认为木马有多么神秘，其实可以简单地说，木马程序就是一个网络上 Client/Server 的概念。以著名的木马程序 Black Orifice（以下简称 BO）来说，它可以搜集信息，运行系统命令重新设置系统，重新定向网络的客户端和服务器端应用程序。只要远程计算机运行了 BO Server 程序，黑客便可重新连接这台主机，运行以上的功能，去控制远程主机和搜集资料。有些功能强大的木马程序，足以成为一个远程控制软件，如有名的"冰河木马"就是其中之一。

以下简单介绍一些木马程序的功能：

1．远程监控

可以控制对方的鼠标、键盘和监视对方屏幕。

2. 记录密码

当用户登录主机时（这里以 Unix 主机来说明），由 login 程序去查看密码，若输入的密码不正确，会出现 Login incorrect 的信息，并要求用户重新输入。Unix 系统上的 login 为了不让其他人窥探到密码，因此密码不会显示在屏幕上，也不会以其他符号如*****代替，虽然提高了安全性，但另一方面来说，用户却也不知道自己是否少打了字或打错字。利用这个特性，早期有一个专门窃取用户密码的木马程序，这个程序在网络上大肆传播，宣称可以缩短输入密码的查看时间，于是有些管理员觉得不错，将这个程序装到自己的系统上，这个程序表面上看起来和一般 login 程序没什么两样，但实际上会将用户的密码记录下来，按照入侵者的指定存在某个目录下，或直接寄回给入侵者。

但这种做法由于程序要同时偷取密码和查看密码，文件也会大很多，可以轻易用校对程序找出来；于是后来演变为木马程序先截取真正的 login，再由木马程序显示 login 提示符号，等用户输入了密码后，木马程序就偷到密码了，之后木马程序还会再产生一个真正的 login 让用户继续进入系统。

3. 取得计算机主机的信息资料

可以取得系统的各种信息（如主机的名称），更改主机名称，设置系统路径和得知系统版本等。

4. 设置系统功能

可以远程关机或重新开机，设置鼠标或是把鼠标隐藏起来，终止系统程序，或是大量耗用主机资源致使系统死机。

5. 远程文件操作

此项是木马程序一般都具有的功能，入侵者可以远程控制对方的文件。

6. 发送信息

这也是一个简单的木马程序功能。

1-2 木马与网络安全

从只是简单地窃取密码开始，黑客的技术不断地改进和发展，在隐藏方面采用了嵌入模式，使得在 Windows NT/2000 下都能达到良好的隐藏效果。在此同时用户也在进步，即使上网不久的人也知道用 NETSTAT 来查看 Port 是否被木马攻占，而木马的 Port 也愈做愈高，愈做愈像是系统本身的正常通讯 Port 了。

1-2-1 微软的玩笑开大了

微软操作系统的安全性一向为人所诟病，才宣布解决了一个漏洞，随即又有新的漏洞

出现，所推出的 VBScript、ActiveX 也是如此，竟能接受未经核准的浏览功能。

1．木马的隐藏技术

微软的系统漏洞之多，是大家所公认的。木马程序制造者发现 Windows 下的汉化软件采用的陷阱技术很适合木马使用，DLL 陷阱技术是一种针对 DLL 的高级编码技术，程序员用特洛伊 DLL 替换已知的系统 DLL，并对所有的函数调用进行过滤。对于正常的调用，使用函数转换器直接转发给被替换的系统 DLL；对于一些事先约定好的特殊情况，DLL 会运行一些相对应的操作。虽然所有的操作都在 DLL 中完成会更加隐蔽，但这也增加了程序编写的难度，这样的木马大多使用 DLL 进行监听。大量特洛伊 DLL 的使用实际上已经危害了 Windows 操作系统的安全和稳定性，听说下一代系统 Windows 2002 已经使用了 DLL 数字签名、校验技术，因此特洛伊 DLL 的时代应该会结束，取代的将是强行嵌入代码技术（插入 DLL、挂接 API、程序的动态替换）。

在服务器端隐藏木马程序可分为两种：一为程序的处理程序仍在进行中，只是让此程序消失在处理程序列表中，这是比较容易实现的，只要把木马服务器端程序注册为一个服务即可，这样程序就会从工作管理员中消失了，因为系统不认为它是一个处理程序，按下 Ctrl + Al t +Delete 时也就看不到这个处理程序。但这种方式只适用于 Windows 9X 系统，至于 Windows NT、Windows 2000 等通过服务管理器的，仍会发现在系统中注册过的服务。另一种则会让程序彻底消失，不以一个处理程序或者应用程序的模式工作。

2．争夺系统控制权

木马程序并不只是处于被动的地位，它们也会进攻，也会出击。Windows NT 下的有些木马程序便是这样的积极者，不仅等待守候、完成命令，而且会利用系统的种种漏洞使之成为系统的管理者——Administrator，或是系统的控制者——System。木马程序在不断的发展中非常熟悉注册表的构造和特点，Windows 2000 有几个注册表的权限漏洞允许非授权的账户改写 Admin，从而强迫 Admin 运行木马程序。此方法实行容易，因此也会被大多数防火墙所找到。利用系统的权限漏洞来改写 Admin 的文件，从而取得系统的权限。

1-2-2 条条网络通你家

无论使用哪种媒介，只要是通信，且传送有价值的信息，就会有安全的顾虑，而在浩瀚的互联网上，只要一上网就是将自己暴露在不安全的环境下，除了病毒的传播外，还有一些新问题，如密码被盗取、信用卡号被盗用等，这样的案例层出不穷。

根据统计，密码被窃取是经常发生的，因为技术性并不是很高，较容易留下痕迹，所以有许多的网站也提供这样的程序。会被盗用除了不小心被猜出来之外，较常见的方式是用演算方式进行“暴力”运算（如 Calymore 程序自己会不断输入密码，直到破解为止），找出可用的密码登录系统为所欲为。在 Unix 系统下，密码表默认是在/etc/passwd，存放了所有使用系统用户的密码，虽然经过了加密处理，但入侵者只要取得此文件，即可用普通的 Crack Jack、John The Ripper 软件加上字典进行对比，破解出系统用户的账号和密码。许多用户为了方便，会选择让 Windows 记忆密码，这也是相当危险的，虽然是以*******代

替，但千万别以为这样就看不出来，因为有一些如 SnadBoy 的程序即可解出，所以宁愿多花点功夫每次都要亲自输入密码。

1-2-3 小心！网络隔墙有耳

在网络上传送数据时，最小的单位为数据包。数据包从一处传到另一处时，可能会经过未加密的公众网络区段，也会经过私人网络区段。如我们要拨号上网到 bbs.ntu.edu.tw 时，会先连上 ISP，再由 ISP 的路由器连接到 bbs.ntu.edu.tw（140.112.1.6），数据包先经过用户的电话线路，再经过公共的互联网，之后到达 140.112.0，这个 Class C 网络最后抵达目标主机。

由于这些网络的传播媒体是共享的，且在同一段网络上采用广播方式传送数据，所以同一个网络区段上的每台主机都可以收到流通的所有数据包，这时网络上所有的数据包都有可能被窃听，而用户也许无法察觉到。

只要将计算机连上互联网，用窃听程序如 Snoop、Sniffer 分析网络上流通的数据包，虽然这些工具原本是用来研究数据包结构、统计分析网络流量、进行网络问题排解，但在有心人利用之下却被用来进行非法的行为。因此对于一些重要的资料，最好是通信的双方皆能传送加密过后的数据包。

1-2-4 更具 Power 的 ICMP 木马

传统的木马程序是利用 TCP/IP 启动命令，但当木马在等待和运行的过程中，会有一个和外界连接的 Port 开着，而在进步中的木马程序便发展出一种摆脱 Port 限制的特洛伊程序。ICMP 的全名是 Internet Control Message Protocol，TCP/UDP/IP 协议若有错误情形发生时，会利用 ICMP 协议来发错误信息。虽然 IP 是利用 ICMP 来发错误信息，但是 ICMP 的数据包却是利用 IP 来包装与传送的，例如大家常用的 Ping 命令就是通过发送接收 ICMP_Echo 和 ICMP_EchoReply 信息来进行网络问题检测的。

ICMP 也是由 Ping 命令得到灵感，由于 ICMP 信息是由系统内部查找或是程序直接处理，而不需经过 Port，所以木马便将自己伪装成一个 Ping 的命令，系统会将 ICMP_EchoReply（Ping 的响应数据包）监听、处理权限交给木马程序，木马接受后分析并从中译出数据码。一般的防火墙会对 ICMP 进行过滤，但对 ICMP_EchoReply 往往不会进行过滤，因为一旦不允许通过，即意味着主机将无法进行 Ping。

第 2 章　黑可黑，非常 High

网络消息：

微软公司正针对有关其 MSN 实时信息传输（IM）业务，就用户名与联系人通讯簿会被人通过失效的 Hotmail 账户盗取的投诉展开紧张的调查。

上周，有用户投诉有人利用失效的 Hotmail 免费邮件账户，来窃取微软现有的 IM 用户的用户名和联系人名单。微软发言人称正在对此“进行深入的调查”。虽然一年多前就有人对这类问题提出过警告。

根据微软的规定，Hotmail 免费电子邮件业务的用户，如果连续三个月不使用其账号，则该账号将被暂时关闭。如果又过了三个月账号仍被闲置，Hotmail 将删除这个账号。然而，据一名用户的投诉，他在原先的 Hotmail 账号因闲置被删除后，又以同一个用户名重新登记了一个账号，却意外地发现自己原先的 IM 联系人名单出现在新登记的账号中。

Cisco 系统公司系统管理员詹姆士·尼尔森说：“假如一名用户是通过他的 Hotmail 账号使用微软的 IM 业务，那么他的账号被删除时，其 IM 联系人名单并没有被清除。如果有人以这个用户名登记了一个账号，就可以得到原先用户的联系人名单。”

2-1　浅谈网络安全的问题

生活平淡无趣，想上网找人聊天吗？在网络上发送邮件、交易血拼吗？

从现在起，请提高警觉心！因为有一双眼睛正监视你的一举一动，并悄悄地从计算机中窃取资料、密码、工作日志、电子邮件……完全都在黑客的掌握之中。如图 2-1 所示。

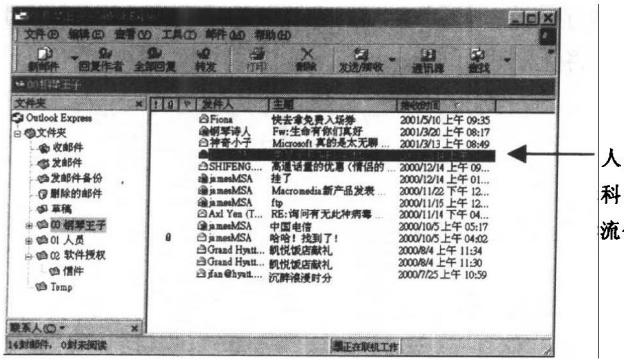


图 2-1（a）

图 2-1（b）

有句话说得好：“网络安全要做得好，惟一的条件就是不要上网”。这是一个矛盾的说法，但这也是一个“事实”，因为我们永远都不能保证，两台计算机相隔之间的网络，百分之百安全、没有黑客的“监听”。在本节中，将为你探讨网络安全问题，介绍目前黑客入侵的手法。

不过，在开始之前，有一个概念必须为你澄清，那就是“入侵”与“破坏”是不同的。不论是哪一个时代的黑客，他们的行径都可以区分为两种，一为“黑客入侵”、一为“黑客破坏”。所谓入侵，是单指进入他人系统中而不被发觉；而破坏，则是恶意地删除数据文件或类似的毁灭性行动。

2-1-1 黑客入侵方式

时代随着科技在改变，黑客的入侵方式也不断在翻新，从早期的密码战、木马，到近来热门的 Sniffer 与系统漏洞，可以看出黑客有多么坚韧不拔的精神。黑客入侵手法是多样、变化的，了解与认识黑客入侵的方法，一来可以保护自己不受侵害，免于遭受黑客入侵而不自知；二来可以防患未然，事先做好严密的保护措施。

1. 常见的黑客入侵方法

（1）暴力猜密码。
（2）Sniffer 拦截数据包。
（3）程序漏洞。
（4）欺骗阴谋法。
（5）代理服务器与网关。

2. 暴力猜密码

密码是进入系统的重要关键（Key），谁拥有访问权的密码，就等于拥有了整个系统。也因为如此，许多人对自己的密码都会加以保护，而黑客要得到密码就显得格外困难了。

那么无法得到，用猜总行了吧，只要写一个小程序，其中利用“循环”的方式，从数字猜到英文，再猜复合的英文与数字，这种暴力猜码的方式，一般都会搭配“密码文件”，通过密码文件里的顺序，依次猜测下来。如图 2-2 所示。

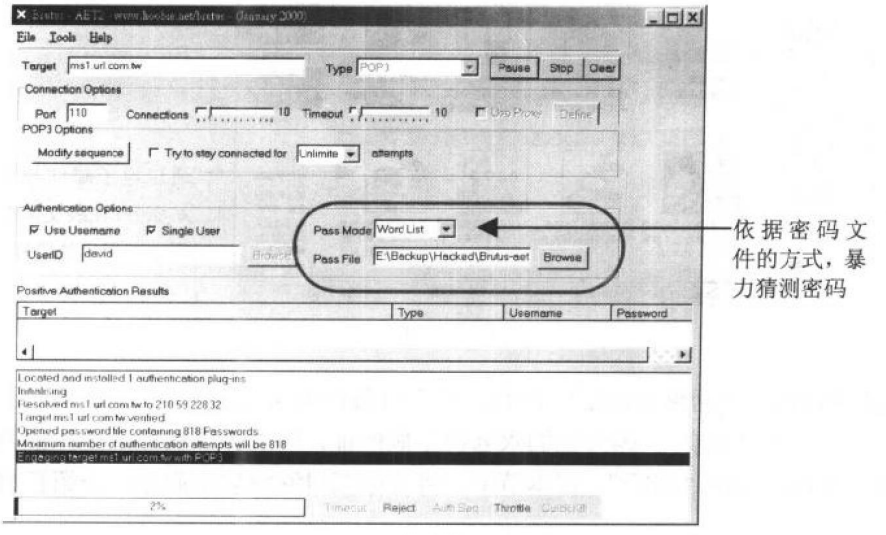


图 2-2

而所谓的“暴力破解法”指的就是一个密码接着一个密码测试，直到猜到密码为止。而其猜测的关键，就在于字典文件里的文字内容。一个好的字典文件，是由许多有意义的字所组成的，当然若要对付没有意义的英文、数字组合，则通过字典文件也会失效。所以，破解密码还是要带点运气的。

补充说明

“字典文件”就是提供给暴力破解法去猜测的密码，而字典文件里的字皆是有意义的字，它也是普通的文本文件。

3. Sniffer 拦截数据包

之前提及的暴力猜密码，不仅耗时费力，若遇上网络大塞车，那么猜密码的时间将会无法预估。事实上，数据文件在网络中传递，可以利用“Sniffer”的方式进行拦截，捕捉网络里流动的数据包，而这一包一包的数据组合起来，就是用户输入的密码、账号，甚至是传递邮件的内容、附件等。如图 2-3 所示。

4. 程序漏洞

黑客入侵，有时候是通过程序的 Bug、漏洞进入的，与前面介绍的入侵方式相比，差别在于前者是有意，后者是无意。程序本身的问题在互联网上有个案例，即是利用 sendmail 及 finger 两个程序的问题，入侵其他在互联网上的计算机，造成许多计算机瘫痪。留后门，