网络安全

安全技巧（十）

小未 主编

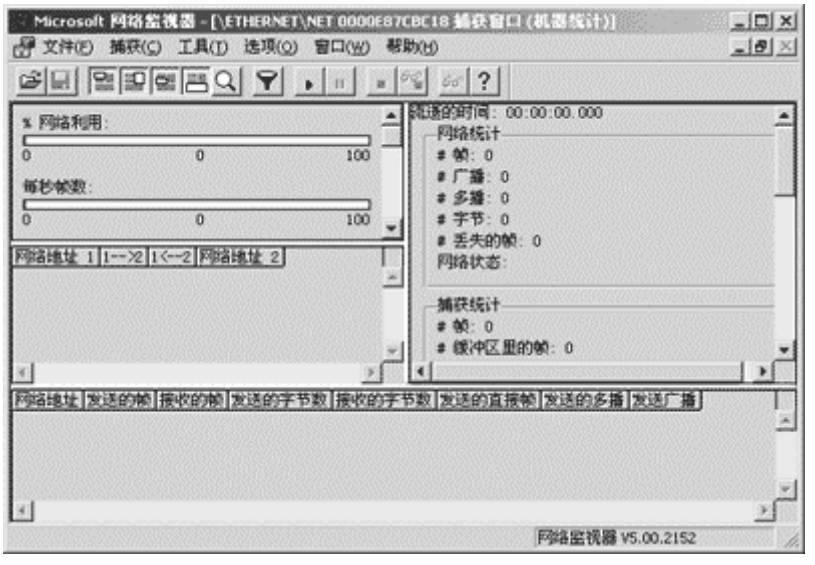
目　录

微软网络监视器的妙用

从前在 Windows98 下为了找一个 Sniffer 翻烂了搜索引擎、问了很多人，才找到一个 SpyNet（现在还有很多网站推荐她的 1.6 版，但是却是要注册的，我破不了。

后来升级后装了 Windows2000Server，发现管理工具里有一个现成的 Sniffer，网络监视器，十分好用。下面我就来向大家介绍一下这个家伙，相信如果你因找不到好的 Sniffer 来学习网络协议的话，你一定会决定装 Win2K 服务器的。

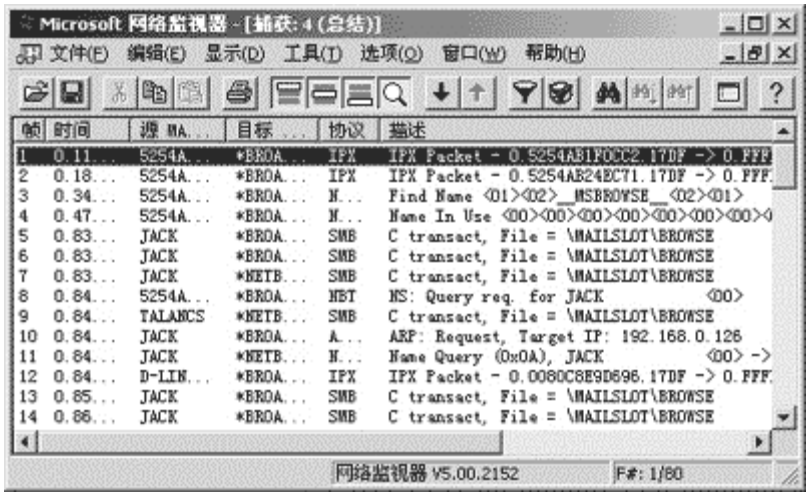
这就是她的主界面：



一按  就开始监视了，很好用吧，或许你想设定只监控某些特点的包，你会发现，她提示你装管理服务器，没办法，找不到系统管理服务器就先这样用吧。

在你按了  后，监视器即开始监视网络信息，我这个这个版本，只能监视本地计算机有关系的包，包括自己发的，发给自己的，和多播、广播的包。但是要注意，如果缓冲区设置超过系统中的可用物理内存，内存交换将导致帧丢失。按一下  就可以停止监视开始分析了。

分析界面如下:



双击每一个帧，就可以看到这个包的详细分析，包括帧、以太、TCP/UDP 等等只要 Windows 能认得出来的都有解释，这十分有助于我们学习协议的详细使用方法。

txt 文件欺骗及防范方法

在众多媒体的宣传报道下，今天的我们都知道了不能轻易打开电子邮件里的可执行文件类的附件，但是显然那些破坏活动的制造者们也看了那些警告防范的文章，他们开始玩一些新的把戏，让您以为那些附件只不过是没有危险的文本文件或是图像文件等就是其手段之一。由于目前大多数人使用的是 windows 系列操作系统，windows 的默认设置是隐藏已知文件扩展名的，而当你去点击那个看上去很友善的文件，那些破坏性的东西就跳出来了。您可能说这我早就知道了，那么下面讲述的.txt 文件的新欺骗方法及原理您知道吗？

假如您收到的邮件附件中有一个看起来是这样的文件：QQ 靓号放送.txt，您是不是认为它肯定是纯文本文件？我要告诉您，不一定！它的实际文件名可以是 QQ 靓号放送.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}。{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B} 在注册表里是 HTML 文件关联的意思。但是存成文件名的时候它并不会显现出来，您看到的就是个.txt 文件，这个文件实际上等同于 QQ 靓号放送.txt.html。那么直接打开这个文件为什么有危险呢？请看如果这个文件的内容如下：

您可能以为它会调用记事本来运行，可是如果您双击它，结果它却调用了 HTML 来运行，并且自动在后台开始格式化 d 盘，同时显示“ Windowsisconfiguringthesystem。Plasedonotinterruptthisprocess。”这样一个对话框

来欺骗您。您看随意打开附件中的.txt 的危险够大了吧？

欺骗实现原理：当您双击这个伪装起来的.txt 时候，由于真正文件扩展名是.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}，也就是.html 文件，于是就会以 html 文件的形式运行，这是它能运行起来的先决条件。

文件内容中的第 2 和第 3 行是它能够产生破坏作用的关键所在。其中第 3 行是破坏行动的执行者，在其中可以加载带有破坏性质的命令。那么第 2 行又是干什么的呢？您可能已经注意到了第 2 行里的“ WSCript ”，对！就是它导演了全幕，它是实际行动总指挥。

WScript 全称 WindowsScriptingHost，它是 Win98 新加进的功能,是一种批次语言/自动执行工具——它所对应的程序“ WScript.exe ”是一个脚本语言解释器，位于 c:\WINDOWS 下，正是它使得脚本可以被执行，就象执行批处理一样。在 WindowsScriptingHost 脚本环境里，预定义了一些对象，通过它自带的几个内置对象，可以实现获取环境变量、创建快捷方式、加载程序、读写注册表等功能。

下面我们通过一个小例子来说明 WindowsScripting Host 功能是如何的强大，使用又是怎样的简单，被有心人利用后的威胁有多大。例如有内容如下的*.vbs 文件：

```
Setso=CreateObject("Scripting.FileSystemObject")
so.GetFile(c:\windows\winipcfg.exe).Copy("e:\winipcfg.exe")
```

就是这么两行就可以拷贝文件到指定地点。第一行是创建一个文件系统对象，第二行前面是打开这个脚本文件，c:\windows\winipcfg.exe 指明是这个程序本身，是一个完整的路径文件名。GetFile 函数获得这个文件，C

opy 函数将这个文件复制到 e 盘根目录下。这也是大多数利用 VBscript 编写的病毒的一个特点。从这里可以看出，禁止了 FileSystemObject 这个对象就可以很有效的控制这种病毒的传播。用 regsvr32scrrun.dll/u 这条命令就可以禁止文件系统对象。

欺骗识别及防范方法：这种带有欺骗性质的.txt 文件显示出来的并不是文本文件的图标，它显示的是未定义文件类型的标志，这是区分它与正常.txt 文件的最好方法。识别的另一个办法是在“按 WEB 页方式”查看时在“我的电脑”左面会显示出其文件名全称，此时可以看到它不是真正的 txt 文件。问题是很多初学者经验不够，老手也可能因为没留意而打开它，在这里再次提醒您，注意您收到的邮件中附件的文件名，不仅要看显示出来的扩展名，还要注意其实际显示的图标是什么。对于附件中别人发来的看起来是.txt 的文件，可以将它下载后用鼠标右键选择“用记事本打开”，这样看会很安全。

让你的 IIS 无懈可击

如果你的电脑新安装了 nt4/win2000 以后，并不是说就可以直接用来作 Internet 服务器了。尽管微软的补丁打了一大堆，但还是有些漏洞。现在我们就简单的谈一下如何使用 IIS 建立一个高安全性能的服务器。

一、以 WindowsNT 的安全机制为基础

1）NT 打 SP6 补丁、2K 打 SP2 补丁。把磁盘的文件系统转换成 NTFS（安装系统的分区可以在安装系统

的时候转换，也可以安装完系统以后，用工具转换）。同时把使用权限里有关 Everyone 的写、修改的权限去掉，关键目录：如 Winnt\Repair 连读的权限也去掉。

2）共享权限的修改。在 NT 下到开始菜单-->程序-->管理工具-->系统策略编辑器，然后打开系统策略里文件菜单里的“打开注册表”修改其中的 windowsNT 网络把其中勾去掉。2K 下可以写个 netsharec$/delete 的 bat 文件，放到机器的启动任务里。

3）为系统管理员账号更名。同时把系统管理员的密码改成强加密：密码长度在 10 位以上，并且密码要包括数字、字母、！等各种字符。

4）废止 TCP/IP 上的 NetBIOS。通过网络属性的绑定选项，废止 NetBIOS 与 TCP/IP 之间的绑定。

5）安装其他服务。应该尽量不在同台服务器上安装数据库的别的服务，如果装了的话，最主要一点是数据库密码不能跟系统的登陆密码一样。

二、设置 IIS 的安全机制

1）解决 IIS4 以及之前的版本受到 D.O.S 攻击会停止服务。运行 Regedt32.exe 在：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w3svc\parameters 增加一个值：ValueName:MaxClientRequestBufferData Type:REG_DWORD 设置为十进制具体数值设置为你想设定的 IIS 允许接受的 URL 最大长度。CNNS 的设置为 256。

2）删除 HTR 脚本映射。

3）将 IISwebserver 下的/_vti_bin 目录设置成禁止远程访问。

4）在 IIS 管理控制台中，点 web 站点，属性，选择

主目录，配置（起始点），应用程序映射，将 htw 与 webhits.dll 的映射删除。

5）如果安装的系统是 2K 的话，安装 Q256888_W2K_SP1_x86_en.EXE。

6）删除:c:\ProgramFiles\CommonFiles\System\Msadc\msadcs.dll。

7）如果不需要使用 IndexServer，禁止或卸载该服务。如果你使用了 IndexServer，请将包含敏感信息的目录的“ Indexthisresource ”的选项禁止。

8）解决 unicode 漏洞：2K 安装 2kunicode.exe、NT 安装 ntunicode86.exe。

经过以上的设置之后,我还是不敢说它就完全安全了,你可不要回去睡大觉呀!不过你可以放松一下了!

微软的产品虽然好用,但是它的漏洞和同类比起来是漏洞最多的一个.作为一个网管要时刻的注意新漏洞的出现,及时的采取相应的措施,做到有备无患!

常见网络安全问题及解决办法

随着计算机的普及和网络技术的迅速发展，人们也越来越依赖于计算机和网络。因此，网络安全应该也必须引起注意。网络安全是一门涉及计算机、网络、通讯、密码、信息安全、应用数学、数论、信息论等多种学科的综合性学科，涉及面极广，而且不断更新和发展。国家对信息产业的扶持，使国内的网络状况逐渐好转，更多的服务器的开通，更快的宽带网得逐渐普及，各种各样的攻击行为在网上也越来越频繁化和简单化。近日的

中美黑客大战，不但不少国内站点被黑，而且黑客技术又大肆传播，潜在的威胁与日俱增。因此，网络安全的严峻性对网络管理员的水平提出了极高的要求。本文将详细介绍各种系统最常见的一些安全问题以及对应的解决办法。

关于 WindowsNT

国内站点中，NT 站点最多，占 91.4%，其余不足 10%的多为类 Unix 系统（如 SunOS、HP-Unix、SCOUnix、Linux、BSDUnix 等）,而恰恰 NT 的漏洞最多。由于微软的技术垄断，NT 的漏洞一般很难迅速、完美地解决。NT 把用户信息和加密口令保存与 SAM 文件中，即安全帐户管理（SecurityAccountsManagement)数据库，由于 NT 的加密过程与 Win9x 一样简单，因此 NT 口令比 Unix(linux)口令更加脆弱，更容易受到一本简单黑客字典的攻击。(NT5.0 已改进了它的加密程序，但国内跑得最多的依然是 NT4.0)。

NT 首当其冲的漏洞就是 SMB 漏洞，其导致 SAM 数据库和其他 NT 服务器及 NT/9x 工作站上的文件可能被 SMB 的后门所共享。SMB(ServerMessageBlock 服务器消息块）是微软早期的 LAN 产品的一种继承协议，即基于 Windows95/98/NT 平台的共享功能。在 LAN 中，共享功能提供了网络中硬盘，CDROM，打印机的资源共享，极大方便了网络的使用。由于 LAN 局限在内部使用，并未引起较大安全问题。当 LAN 连上因特网，成为一个子网络时，人们通常还是认为，共享功能仅限于 LAN 使用，其实不然，通过因特网，是可以访问到 LAN 中的共享资源。共享资源有两种访问方式，一种是只读方式，另一种是完全访问方式。通常基于方便使用

的考虑，共享资源都没有设置口令，而且，有些还打开了完全访问方式。这样，一个菜鸟黑客都可以利用 Internet 上俯拾皆是的 SMB 黑客工具，来窃取文件，删除磁盘，甚至上传木马，以达到长期、更进一步控制的目的。仅我知道的此类软件就有老掉牙的 Logion、Redbutton 和 NetHackerII。用这些软件访问 LAN 不需要 Administrator 访问权或者交互式访问权。NT 在安装后，每个磁盘都会缺省地被设置成共享，这时后，Internet 和 LAN 上的任何人都可以用命令行方式连接服务器。如在开始-运行里键入“ \\IPADDRESS\C$,\\IPADDRESS\D&…… ”或在 Dos 下连接。当前。对于使用 SMB 进行 NT 组网，还没有任何其他可选的方法。

建议：安装 NT 后，立即修改磁盘共享属性；严格控制共享，请加上复杂的口令；打印服务器应认真对待，任何人都可以通过 SMB 漏洞将你的打印驱动替换成木马或夹入病毒；安装防火墙，截止从端口 135 到 142 的所有 TCP 和 UDP 连接，这样有利于控制，其中包括对基于 RPC 工作于 135 端口的安全漏洞的控制。当然，最安全的方法是利用代理（Proxy）来限制或者完全拒绝网络上基于 SMB 的连接；同时在内部路由器上设置 ACL，在各个独立子网之间，截止端口 135 至 142。

另一大漏洞就是注册表访问漏洞。NT 的缺省 Registry 权限有很多不恰当之处。第一，Registry 的缺省权限设置是对 Everyone（所有人）的 FullControl（完全控制）和 Create（创建），这可能导致注册表文件被不知情用户或恶意用户修改、删除或替换。第二，NT 的缺省状态下是允许用户远程访问 NT 的注册表。这将导致严重的安全隐患。

建议：立即关掉“远程注册表造访”，使用第三方的工具软件如 EnterpriseAdministrator 来管理注册表，必要时将其锁住。或手动修改注册表——在 HKEY_Local_Machine\System\CurrentControlSet\Control\SecurePipeServer 下添加 Winreg 项(Reg_SZ 类型)，再在其下添加 Description 值（Reg_SZ 类型），输入字符串“ Registrysever", 重启计算机。

NT 的进程定期处理机制有较大漏洞。NT 允许非特权用户运行某些特别的程序，导致 NT 系统崩溃或者挂起。CPUHOG 是一个只有 5 行的小程序，它可以使 NT 挂起；NTCrash 与前者类似，这类软件在 Internet 上到处可见。一些扫描器也可以使 NT 拒绝服务，如经典的 SATAN 和 InternetScanner,它们都可以使 NT 崩溃。甚至用一条简单的 Ping 命令（对，就是 Win9x/Nt 中的 Ping）也可以服务器重启。如“ Ping-l65524host.domain.com ”。究其原因，在于 NT 对较大的 ICMP 包是很脆弱的，如果向 NT 发一条指定包大小为 64K 的 Ping 命令，NT 的 TCP/IPStack 将不会正常工作。此种情况会使系统离线工作，直至重启。

建议：赶快去下载 ServicePack6，立即安装。

帐户设置不合理也是人为的安全因素，如果和 NT 密码的脆弱性联合起来，又是一个严重的隐患。通常入侵者最感兴趣的是 Administrator 帐户，次之是 Guest 帐户。因此，必须严格地设置域和帐户。

建议：必须设置两个或两个以上的系统管理员帐户，以免万一入侵者已得到最高权限并将口令更改。并且将原 Administrator 帐户改名，加上复杂的口令，再设置一个没有任何权限的假 Administrator 帐户，以欺骗入侵者；

取消 Guest 帐户或者加上复杂的口令；设置口令尝试次数上限，达到即锁住该帐户，以防止穷举口令；关注系统日志，对大量 Login 失败记录应保持警惕。

LAN 中的不友好用户和恶意用户也应注意。通常 LAN 中的用户得到管理员权限的成功概率高达 70%，而其他用户则不到 5%，因为本网用户通常较熟悉管理员的工作习惯，而且穷举口令在局域网中也比从互联网上快得多（LAN 中 100 次/秒，Internet 中 3-5 次/秒）。“最危险的敌人通常都在你身边”，此类的黑客工具举不胜举，如 NTRecover、NTLocksmith(NT 锁匠，这名字倒是恰如其分)、Getadmin、IKS、L0phtCrack……另外，网络监听（也叫嗅查器 Sniffer）也是 LAN 中常用的窃密方法。因为一般公司都是使用共享式的 HUB，所以只要将网卡接口设置为监听模式即可，通常可以截获本段网络中传送的信息流，加以分析，从中得到密码。我用 NetHackerII 试着监听了本段局域网仅两分钟，就得到了一个叫“super99”的明文共享口令；而密文口令，可以保存成 SMB 文本，送 L0phtCracker 解密。L0phtCracker2.52 在 48 小时内，几乎能解 90%以上的密码（当然要一个好字典哦:-)）。现在的入侵者在服务器久攻不下后，会用 IP 扫描器扫描服务器所在网段（如冯志宏大侠的“月光搜索”），得到本网段的工作站的 IP，然后挨个尝试，找出最脆弱的一台攻击，得手后即开始监听，伺机窃得管理员口令。而且在宽带网逐渐普及的今天，攻击的速度也越来越快。可能原来需要一个月跑出来的口令，现在只需一天或几小时。

建议：采用 SwitchHUB 后就只能监听本网段；严格设定域和工作组，用拓扑结构将各个域分开。

另外，Modem 拨入式访问也应引起注意。不要将电话号码透露给任何人,不要将记有号码的介质随意放置，并要给此种访问加上口令。NT 在默认状况下用紧急修复盘更新后，整个 SAM 数据库会被复制到%system%repair\sam._下，而且对所有人可读。因此在修复后，立即将其改为对所有人不可读。

关于泛 Unix

NT 由于界面友好，操作简单，被中小型企业广泛采用；而 Unix 由于对管理人员要求较高，常常用于大型企业和 ISP。因此，若此类服务器被摧毁，损失将是惊人的。

Unix 系统中的/etc/passwd 文件是整个系统中最重要的文件，它包含了每个用户的信息（加密后的口令也可能存与/etc/shadow 文件中）。它每一行分为 7 个部分，依次为用户登录名，加密过的口令，用户号，用户组号，用户全名，用户主目录和用户所用的 Shell 程序，其中用户号（UID）和用户组号（GID)用于 Unix 系统唯一地标识用户和同组用户及用户的访问权限。这个文件是用 DES 不可逆算法加密的，只能用 John 之类的软件穷举，因此，此文件成为入侵者的首要目标。通常黑客用 FTP 匿名登录后将 passwdGet 回去，就用 John 开始跑了。所以一定要把此文件设为不可读不可写。另注意，opasswd 或 passwd.old 是 passwd 的备份，它们可能存在，如果存在，一定也要设为不可读不可写

文件许可权也是应高度注意的问题。用 ls-l 可以看到文件的权限。r 表示可读，w 表示可写，x 表示可执行；第一个 rwx 表示文件属主的访问权限，第二个 rwx 表示文件属主同组用户的访问权限，第三个 rwx 表示其他用

户的访问权限。改变文件的属主和组名可用 chown 和 chgrp,但修改后原属主和组名就无法修改回来了。用 ls-l 看时，目录前面有个 d，在 Unix 中，目录也是文件，所以目录许可也类似与文件许可。

用户目录下的.profile 文件在用户登录时就被执行，若此文件对其他人是可写的则系统的任何用户都能修改此文件，比如上传木马，加入后门。如“ echo"++">.rhosts ”就可随意进出其他用户帐号，再开始攻击，从而嫁祸他人。应设置用户 ID 许可和同组用户 ID 许可；并将 umask 命令加入每个用户的.profile 文件，以避免特络依木马攻击和各种模拟 Login 的诱骗。同时应多用 ls-l 查看自己的目录，包括以.开头的文件。任何不属于自己但存在于自己目录的文件应立即引起怀疑和追究。

最好不设匿名帐户或来宾帐户（anonymouse&guest）如果一定要设，请在/etc/passwd 中将其 shell 设为/bin/failure，使其不能访问任何 shell。（注意：Linux 中是设为/bin/false）。打开 chroot（如 chroot-s）,使其访问的文件限定在一定目录下。

作为 root 登录后，应时刻保持清醒，知道自己下一步该做什么，因为你的一点微小的疏忽都可能给整个系统带来不良后果，甚至导致系统崩溃。尽量少用 root 登录，而以具有同样权限的其他帐户登录，或用普通帐户登录后再用 su 命令取得管理员权限。这样做是为了避免可能潜在的嗅探器监听和加载木马。给你的 root 帐户加上足够复杂的口令，并定期更换。

Unix 可执行文件的目录如/bin 可由所有的用户进行读访问,这样用户就可以从可执行文件中得到其版本号，从而知道它会有什么样的漏洞。如从 Telnet 就可以知道

sendmail 的版本号。禁止对某些文件的访问虽不能完全禁止黑客地攻击，但至少可以使攻击变得更加困难。

如果是 SunOS 系统，请及时关注 Sun 的补丁信息，因为 SunOS 系统被侵入的事件较多，而且国内绝大部分重要的网络(国家政府部门，邮电通信，教育部门等)都采用 SunOS 系统。据报道，有 30%上有严重的 root 级安全问题，如最经典的例子：SunOSV4 安装时会创建一个/rhosts 文件，这个文件允许 Internet 上的任何人可以登录主机并获得超级用户权限。SUN 的本意是方便管理员从网上进行安装，但也为入侵者大开其门。比较新的例子有 SunOS 的 rpc.ttdbserver 存在巨大漏洞，可以使任何人远程登录取得 root 级权限并不需要何口令，接着一条 rm-fr*的命令就可以……建议网络管理员去下载最新的补丁。并且注意的是，通常管理员对核心主机非常关注，会及时补上补丁，但同网络内的其他主机的管理却没有跟上，入侵者虽然通常无法直接突破核心主机，但往往通过这一点，先突破附近的电脑，进入 LAN 网络，在利用嗅探器等方式监视 LAN，获取通向服务器的途径。所以，同网段的机器都应该同等级重视。

这里将常见的系统漏洞的版本号总结一下，如果您的版本号与此相同，请立即升级系统或安装补丁程序。

Linux1.2.13 可以利用 CGI 轻松获得 root 权限（这个太老了吧！）

XFree863.1.2 的某个漏洞可使其他替罪羊代为删除任何文件

Sendmail8.7-8.8.2forLinux,FreeBSD 有 root 级漏洞

SunOSVersion4.0 有 root 级漏洞

关于 CGI 等

CGI 是主页安全漏洞的主要来源。CGI(COMMOMGATEINTERFACE)是外部应用程序与 WEB 服务器交互的一个标准接口,它可以完成客户端与服务器的交互操作。CGI 带来了动态的网页服务,但是 INTERNET 的宗旨是面向每个人的，任何人可在任何时候任意多次通过 INTERNET 访问某 WEB 服务器，而这些特性又会给 INTERNET 带来安全上的问题。CGI 程序设计不当,就可能暴露未经授权的数据,例如,一个最早的 CGI 漏洞:在浏览器里输入

http://www.xxxx.xxxx.com/cgi-bin/phf?Qalias=x%0a/bin/cat/etc/passwd 就可以看到 Unix 服务器的 passwd 文件。

/msads/Samples/SELECTOR/showcode.asp 可以看到 NT 服务器上的任何文件。这些 root 级漏洞几乎均来自与用户的交互，这种交互性在给主页带来活力的同时，成为 Web 服务器的一个潜在危险。具有破坏性的数据可以从多种渠道进入服务器，客户端可以设计自己的数据录入方式，数据内容，然后调用服务器端的 CGI 程序。如有的留言板可以用……的方法屏蔽 CGI，使它支持超文本，然后五花八门的 Java 炸弹、色情图片、色情链接搞得留言板乌烟瘴气。又如可以由客户端用户任意设定数据的长度，如果用户恶意地设置超长数据，结果是系统挂起，甚至导致瘫痪。

那么究竟应如何防止这些数据的入侵呢?首先服务器应对输入数据的长度有严格限制，在使用 POST 方法时，环境变量 CONTENT－LENGTH 能确保合理的数据长度，对总的数据长度和单个变量的数据长度都应有检查功能；另外，GET 方法虽可以自动设定长度，但不要