网络安全

安全技巧（十二）

小未 主编

目　录

WINDOWS 下的 IP 欺骗：终极指南

目前有很多有关 ip 地址欺骗的思考，特别是在 WINDOWS 环境下。这听起来是个奇妙的注意，但不全是像看起来那样。在这篇指南里将讨论着这问题并回答最根本的问题：这可能吗？

首先，在网上你的 IP 地址并不是唯一标明你身份的东西。还有其他要素要考虑，比如你的域名和你的身份。人们并不是只有通过你的 IP 地址才知道你是谁。即使你已经实现了欺骗，你也并不是完全不能被发现的。有许多其它方法可用来获得你的机器名和 IP 地址，例如下面的 VB 脚本：Request.ServerVariables("REMOTE_ADDR");

这可以用来确定你是谁。在很多站点上都用了这条语句，或类似的语句（当然这并不会让你知道），其中有些是非常仔细的，用来确保你不会做任何有害的事，但是其他纪录却有另外的目的，例如用来扫描 NETBUS

-=个人观点-=

你仍然可以通过匿名方式浏览站点，只要把你的脚本和 JAVA 关掉就可以了，并且在填写 CGI 和 ASP 表格是要格外小心。

现在回到主题：在 WINDOWS 下可能通过 IP/域名欺骗而达到匿名的目的吗？说实话，并没有一个直接的答案。不能直接通过 WINDOWS...所有那些说可以将你隐藏的程序都是没有用的。这是因为 WINDOWS 下的客户/服务器模式。你不可以简单的告诉服务器你的域名和

IP 地址。DUP 和 WINSOCK 不允许这么做。

-=个人观点-=

事实上，有一种方法可以直接在 WINDOWS 下实现欺骗...或者说在理论上有一个方法。这是一个高级的方法，并需要 x86 汇编和拨号网络的知识。你可以和你的 MODEN 交谈并且告诉她你想要的 IP，尽管如此，我不肯定是否域名也可以。我所要说的是在 x86 体系结构下，MODEN 可以在 INT14H 被发现，并且可以在 DUP 协议下发现一个叫"defaultip"的部分。

所以...假如你不能再 WINDOWS 下直接的实现欺骗...你会做什么？好吧，如果你进入了一个 shellaccount 并连上了网络，你将不再使用你的 ISP 的域名，它将会是你的 shell 提供者的，例如 jdoe@shellyeah.org。还有其他方法，例如使用代理服务器。

-=个人观点-=

代理服务器类似于防火墙，它可以控制在服务器上进出的数据。你有可能正在使用代理服务器而并不知道。你可以在控制面版下的 internetsettings 下查看到相关内容。

如果一个代理服务器可以控制进出的数据，那它可以对 IP 作同样的工作吗？答案是肯定的 !但是你很难找到一个那样的代理服务器。有一种基于 CGI 的代理在 www.jmarshall.com...它可以让你彻底的匿名...你可以在 www.schematic.org 上试一下。但那仅仅是表面上的...并且只有这一个站点。能够让你实现 IP 欺骗是一件不太可能的事。即使你真的发现了一个方法，肯定还有其他人会发现某种方法来查出你真实的 IP 是什么，除非有一种非常强大的加密技术。

-=个人观点-=

有一种叫 Freedom 的产品可以让你实现匿名，它可以让你使用数个代理服务器并且加密你的真实身份。不幸的是，作为这个产品 beta 版的测试者，我发现它把一些原本很简单就能完成的工作做得很复杂。你可以在 www.zeroknowledge.com 下载这个产品 30 天的试用版。所以基本上,如果你想实现 IP 欺骗...删了你的 WINDOWS！UNIX 系统的实现方式不同，并且在理论上完全有可能做到 IP 欺骗。但是要记住，IP 欺骗并不能使你匿名。你必须考虑的更多。好吧，就写这么多，下面是一些注意点，同时欢迎和我交流 kaspa@hfactorx.org

-=注意点-=

*尝试学习有关拨号网络（DialUpNetworking）的知识，在网络上可以找到很多相关内容。

*如果你坚持要在 WINDOWS 下做 IP 欺骗，那最好先学习一下有关 MODEM 的原理技术。在 x86 汇编下可以找到指导。

*尝试一下 UNIX 在 www.linux.org,www.freebsd.org,www.openbsd.com,www.netbsd.org.....可以找到。

也谈网管软件的安全问题

前些日子看了电脑报的有关网管软件安全问题，我也是常用美萍软件的。试一下确实存在的问题，好在美萍又推出了新的版本 7.61，解决了此问题。但是我在使用新美萍后，发现设置密大小写码后不能正常使用。系统不能设置，也退不出美萍。没了密码，我一直在想办

法，用以前文章提到的方法没有用。后来在无意中使用了 win+f 查找功能,输入盘符。一搜索，嘿嘿全都出来，赶紧随便找了一个目录，打开后，再点上一步，所有的该盘上东西全出来了（原来盘符是隐藏的），如果没有隐藏盘符，还有一个更好的方法。就是打开一个网页，点菜单栏上的查看栏下的浏览栏再点文件夹，居然有了资源管理器。再找到美萍的目录，随便改名后重新启动。系统找不到美萍的 DLL 文件，按任意键继续启动，终于见到了好久没见到的既陌生又熟悉的画面。赶紧运行注册表删除密码部分，改回美萍目录。启动美萍后没有密码了，经多次试验，原来是用 shift 键输大小写作的怪。

经过这次经历后,我想网管软件也有不安全的地方，就多方面测试一下。在通过网页查看源文件，打开一个记事本。修改启动文件，也能达到所要修改的目的。如修改 Msdos.sys 文件。在 AUTOEXEC.BAT、win.ini、winstar.bat 等一些文件中加入所要运行的文件也能成功。另外还有一个问题，就是下载软件。虽然美萍有限制功能，但只要在要下载的文件上单击右键，点一下目标另存为即可，想要的软件就来了。下载完毕后打开、安装就可以用了。如果不能用就用上面的方法查找它，再双击一下就行了。

最后劝大家使用网管软件，要配合一些辅助软件使用，才能使电脑更安全。

修改 TerminalServer 默认的端口

前段时间国内闹的沸沸扬扬、一时间人人都成黑客

红客什么的那个著名的中文输入法漏洞

加上 Windows2000 **里面全选就会安装上去的** TerminalServer **组合成的超必杀中文** 2K **入侵完全解决方案曾经让无数英雄好汉都统统挂掉。。**

一个很大的原因是著名的 TerminalServer **所开的端口（**PORT:3389**）默认情况下是无法修改的。**

于是我们要修改 TerminalServer **的端口**

总共有两个步骤：一是修改服务器端的端口设置；二是修改客户端连接时的端口设置

look:

一、修改服务器端的端口设置

注册表有 2 **个地方需要修改**

第一个地方：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp]

PortNumber **值，默认是** 3389**，修改成所希望的端口，比如** 6000

第二个地方：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp]

PortNumber **值，默认是** 3389**，修改成所希望的端口，比如** 6000

现在这样就可以了。重启系统吧。

注意：事实上，只修改第二处也是可以的。另外，第二处的标准联结应该是

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\

表示具体的某个 RDP-TCP **连结。**

重启过后看看端口有没有改……

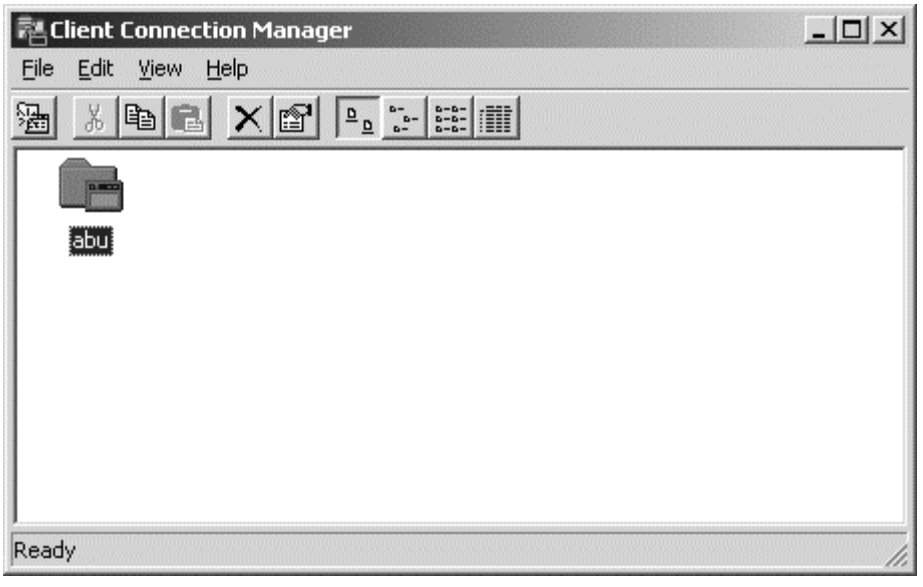
很明显改了。

二、修改客户端连接时的端口设置

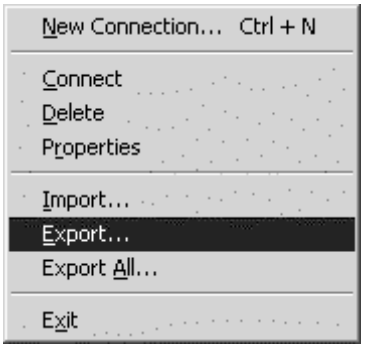
打开 TerminalServer **的客户端连结管理器**

创建一个连结，就和平时一样：

完成后看见如下：



激活它并选择 Export**（导出）成文件**



打开记事本或者 UltraEdit **修改这个**.cns **文件**

```
[abu]
WinPosStr=0,1,0,0,783,550
Expand=1
Smooth Scrolling=0
Shadow Bitmap Enabled=1
Dedicated Terminal=0
Server Port=5000
Enable Mouse=1
Disable CTRL+ALT+DEL=1
DoubleClick Detect=0
Full Screen Hotkey=3
Icon Index=0
Desktop Size ID=1
Screen Mode ID=1
```

看见激活行了么？

是的，修改 ServerPort=3389 这一行，改为自定义的端口。保存。

然后再从 TerminalServer 的客户端连结管理器里面选择导入

导入那个修改过的.cns 文件。

双击该文件……

于是。。搞定！

在这里有一些 tips 说说

开始自己连的时候怎么也连不上,步骤都没有问题。后来才发现，我的 TerminalServer 客户端似乎……

果然！TerminalServer 客户端有很多个版本。原先使用的是 MSI 版本中的 32 位的版本，后来发现居然还有一个叫做 net 版的客户端程序。于是搞来安装……

一连通过！

移动 IP 原理

移动 IP 是一种正在计划中的标准协议，就象 TCP 一样，它建立在 IP 基础之上，并且其移动性对应用程序

和高层协议来说是透明的。

尽管 Internet 为我们提供了一种对全球范围内的各种信息资源的访问手段，但通常的情况是，如果我们不在自己熟悉的某些地方--家中、办公室或学校，我们还是无法从这种手段中获得好处。然而，象个人数字助理、手持设备和蜂窝电话等各种提供 IP 连接方法的无线设备的不断增长，正开始改变我们对 Internet 的看法。

要理解 IP 现行的连接方式与未来可能的连接方式之间的差异，我们可以回顾在过去的二十年间所发生的电话技术向着移动方向的发展变化。与此相似，在网络计算领域中，从对定点连接的依赖性向移动连接的灵活性的过渡刚刚开始。

不应把移动网络计算和我们今天已拥有的便携网络计算混为一谈。对移动网络计算来说，当用户改变计算机与 Internet 的连接点时，其计算活动不会受到影响。相反，所有需要的重新连接都将自动完成，并且是非交互式的。

真正的移动计算具有许多优点。正如蜂窝电话技术给我们带来的完成工作时的自由，能够在任何时间、任何地点对 Internet 进行有效的访问，将使我们摆脱束缚，把我们从办公桌前解放出来。能够携带整个计算环境的能力，不仅使灵活性得以增强，而且可以从根本上改变我们现行的工作方式。如果我们在移动过程中仍能访问 Internet，那么不论我们走到哪里，我们都将拥有一种手段用来建立新的计算环境。而那些本身对移动能力不怎么感兴趣的人，仍然能够从这种能力中获得好处--当他们重新连接时，能够恢复先前的应用。这一点对无线办公环境来说特别方便，在这种环境下，连接点之间的界

线并不明显并且常常是不可见的。

在某些重要的方面，移动网络计算的发展变化将会不同于电话技术的发展变化。通常，电话连接的终点是人，而有关计算机的应用可能包括机器之间无人干预的交互。关于这一点的明显例子是在飞机、轮船或汽车上的移动计算设备。移动网络计算或许也要依赖于某些定位设备，

比如卫星全球定位系统，用来与 Internet 无线访问设备协同工作。

另一个差异也许是人们的接受速度。移动电话用了许多年的时间才变的足够的廉价轻巧而被人们认为能带来方便。由于象个人数字助理和袖珍助手(PocketOrganizer)等无线计算设备已为用户所接受，因而，移动计算也许会更快地流行起来。

然而，在移动网络计算被广泛使用之前，还有一些技术障碍需要克服。最主要的是依据 IP 地址，使用目前 Internet 联网所使用的 IP 协议，将包发送到目的地的方法。IP 地址与固定的网络位置相联系，这一点非常类似于一部普通电话机与墙上的一个插座物理地连接在一起。如果包的发送目的地是一个移动节点，那么这将意味着，随着该节点的移动而产生的每一个新连接点将与一个新的网络号或是一个新的 IP 地址相联系，从而使透明的移动能力成为不可能。

由 Internet 工程任务组(IETF)内的一个工作小组提出的移动 IP 协议是一种标准。其设计目标就是要解决上述问题，其方法是允许移动节点使用两种 IP 地址：一个固定的主地址和一个随新连接点的产生而产生的 care-of 地址。

关于移动计算有许多令人感兴趣的问题，很明显，移动 IP 协议要为它们提供一种方法。在 Web 上进行与移动 IP 有关的条目的快速搜索，将得到超过 6 万条的议题，几乎让你无从选择。移动 IP 直接或间接地构成了当前许多科研成果或产品的基础。例如，蜂窝数字数据包(CDPD)就是基于该协议先前的草议案而建立其广泛使用的通讯底层结构的。此外，许多主要的路由器销售商都已经开发出了移动 IP 的支持工具。

从复杂的 Internet 市场来看，移动 IP 的前景尚不明朗，一些技术问题仍然存在，其中最主要的是安全性问题。然而，一旦安全性问题得以解决，犹豫不定的用户们将会喜欢上移动 IP 许诺给他们的便利：无缝的连接、自由的漫游和对应用程序的有效的透明性。

八种扫描器-系统的大敌

⑴NSS（网络安全扫描器）

■Sendmail

■匿名 FTP

■NFS 出口

■TFTP

■Hosts.equiv

■Xhost

注：除非你拥有最高特权，否则 NSS 不允许你执行 Hosts.equiv。

利用 NSS，用户可以增加更强大的功能，其中包括：

■AppleTalk 扫描

■Novell 扫描

■LAN 管理员扫描

■可扫描子网

简单地说，NSS 执行的进程包括：

■取得指定域的列表或报告，该域原本不存在这类列表

■用 Ping 命令确定指定主机是否是活性的

■扫描目标主机的端口

■报告指定地址的漏洞

尽管没有详尽讨论 NSS，但我在这里要说明一些次要的问题：

■在对 NSS 进行解压缩后，不能立即运行 NSS，需要对它进行一些修改，必须设置一些环境变量，以适应你的机器配置。主要变量包括：

■$TmpDir_NSS 使用的临时目录

■$YPX-ypx 应用程序的目录

■$PING_可执行的 ping 命令的目录

■$XWININFO_xwininfo 的目录

提示：如果你隐藏了 Perlinclude 目录（目录中有 Perlinclude 文件），并且在 PATH 环境变量中没有包含该目录，你需要加上这个目录；同时，用户应该注意 NSS 需要 ftplib.pl 库函数。NSS 具有并行能力，可以在许多工作站之间进行分布式扫描。而且，它可以使进程分支。在资源有限的机器上运行 NSS（或未经允许运行 NSS）应该避免这种情况，在代码中有这方面的选项设置。

你可在下面地址找到 NSS 拷贝。http://www.giga.or.at/pub/hacker/unix

⑵Strobe（超级优化 TCP 端口检测程序）

strobe 是一个 TCP 端口扫描器，它可以记录指定机器的所有开放端口。strobe 运行速度快（其作者声称在适中的时间内，便可扫描整个一个国家的机器）。

strobe 的主要特点是，它能快速识别指定机器上正在运行什么服务。strobe 的主要不足是这类信息是很有限的，一次 strobe 攻击充其量可以提供给“入侵者”一个粗略的指南，告诉什么服务可以被攻击。但是，strobe 用扩展的行命令选项弥补了这个不足。比如，在用大量指定端口扫描主机时，你可以禁止所有重复的端口描述。（仅打印首次端口定义）其他选项包括：

■定义起始和终止端口

■定义在多长时间内接收不到端口或主机响应，便终止这次扫描。

■定义使用的 socket 号码

■定义 strobe 要捕捉的目标主机的文件

在如下地址可以找到 strobe 的拷贝：http://sunsite.kth.se/linux/system/network/admin/

提示：在你获得 strobe 的同时，必然获得手册页面，这对于 Solaris2.3 是一个明显的问题，为了防止发生问题，你必须禁止使用 getpeername()。在行命令中加入-g 标志就可以实现这一目的。

同时，尽管 strobe 没有对远程主机进行广泛测试，但它留下的痕迹与早期的 ISS 一样明显，被 strobe 扫描过的主机会知道这一切（这非常象在/var/adm/messages 文件中执行连接请求）。

⑶SATAN（安全管理员的网络分析工具）

SATAN 是为 UNIX 设计的，它主要是用 C 和 Perl 语言编写的（为了用户界面的友好性，还用了一些 HT

ML 技术）。它能在许多类 UNIX 平台上运行，有些根本不需要移植，而在其他平台上也只是略作移植。

注意：在 Linux 上运行 SATAN 有一个特殊问题，应用于原系统的某些规则在 Linus 平台上会引起系统失效的致命缺陷；在 tcp-scan 模块中实现 select()调用也会产生问题；最后要说的是，如果用户扫描一个完整子网，则会引进反向 fping 爆炸，也即套接字（socket）缓冲溢出。但是，有一个站点不但包含了用于 Linux 的、改进的 SATAN 二进制代码，还包含了 diff 文件，这些条款可以在 ftp.lod.com

上发现，或者可以直接从 Sun 站点（sunsite.unc.edu）取得 diff 文件：

/pub/linux/system/network/admin/satan-linux.1.1.1.diff.gz

SATAN 用于扫描远程主机的许多已知的漏洞，其中包括，但并不限于下列这些漏洞：

■FTPD 脆弱性和可写的 FTP 目录

■NFS 脆弱性

■NIS 脆弱性

■RSH 脆弱性

■Sendmail

■X 服务器脆弱性

你可在下面地址中获得 SATAN 的拷贝：http://www.fish.com

安装过程

SATAN 的安装和其他应用程序一样，每个平台上的 SATAN 目录可能略有不同，但一般都是/satan-1.1.1。安装的第一步（在阅读了使用文档说明后）是运行 Perl 程