ADSL防御黑客攻击的十大方法

ADSL防御黑客攻击的十大方法

[繁體中文] | 文章类别：安全在线 | 文章等级： | 发表日期：2005-5-11 星期三

网站计数器 | 魔法表情申请 | 源码下载 | 休闲游戏 | 精彩博客 | Html2Js

转自:动态网制作指南 www.knowsky.com

目前，使用ADSL的用户越来越多，由于ADSL用户在线时间长、速度快，因此成为黑客们的攻击目标。现在网上出现了各种越来越详细的“IP地址库”，要知道一些ADSL用户的IP是非常容易的事情。要怎么保卫自己的网络安全呢？不妨看看以下方法。

一、取消文件夹隐藏共享

如果你使用了Windows 2000/XP系统，右键单击C盘或者其他盘，选择"共享"，你会惊奇地发现它已经被设置为“共享该文件夹”，而在“网上邻居”中却看不到这些内容，这是怎么回事呢？

原来，在默认状态下，Windows 2000/XP会开启所有分区的隐藏共享，从“控制面板/管理工具/计算机管理”窗口下选择“系统工具/共享文件夹/共享”，就可以看到硬盘上的每个分区名后面都加了一个“$”。但是只要键入“\\计算机名或者IP\C$”，系统就会询问用户名和密码，遗憾的是，大多数个人用户系统Administrator的密码都为空，入侵者可以轻易看到C盘的内容，这就给网络安全带来了极大的隐患。

怎么来消除默认共享呢？方法很简单，打开注册表编辑器，进入“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Sevices\Lanmanworkstation\parameters”，新建一个名为“AutoShareWKs”的双字节值，并将其值设为“0”，然后重新启动电脑，这样共享就取消了。

二、拒绝恶意代码

恶意网页成了宽带的最大威胁之一。以前使用Modem，因为打开网页的速度慢，在完全打开前关闭恶意网页还有避免中招的可能性。现在宽带的速度这么快，所以很容易就被恶意网页攻击。

一般恶意网页都是因为加入了用编写的恶意代码才有破坏力的。这些恶意代码就相当于一些小程序，只要打开该网页就会被运行。所以要避免恶意网页的攻击只要禁止这些恶意代码的运行就可以了。

运行IE浏览器，点击“工具/Internet选项/安全/自定义级别”，将安全级别定义为“安全级-高”，对“ActiveX控件和插件”中第2、3项设置为“禁用”，其它项设置为“提示”，之后点击“确定”。这样设置后，当你使用IE浏览网页时，就能有效避免恶意网页中恶意代码的攻击。

三、封死黑客的“后门”

俗话说“无风不起浪”，既然黑客能进入，那说明系统一定存在为他们打开的“后门”，只要堵死这个后门，让黑客无处下手，便无后顾之忧！

1.删掉不必要的协议

对于服务器和主机来说，一般只安装TCP/IP协议就够了。鼠标右击“网络邻居”，选择“属性”，再鼠标右击“本地连接”，选择“属性”，卸载不必要的协议。其中NETBIOS是很多安全缺陷的根源，对于不需要提供文件和打印共享的主机，还可以将绑定在TCP/IP协议的NETBIOS关闭，避免针对NETBIOS的攻击。选择“TCP/IP协议/属性/高级”，进入“高级TCP/IP设置”对话框，选择“WINS”标签，勾选“禁用TCP/IP上的NETBIOS”一项，关闭NETBIOS。

2.关闭“文件和打印共享”

文件和打印共享应该是一个非常有用的功能，但在不需要它的时候，也是黑客入侵的很好的安全漏洞。所以在没有必要“文件和打印共享”的情况下，我们可以将它关闭。用鼠标右击“网络邻居”，选择“属性”，然后单击“文件和打印共享”按钮，将弹出的“文件和打印共享”对话框中的两个复选框中的钩去掉即可。

虽然“文件和打印共享”关闭了，但是还不能确保安全，还要修改注册表，禁止它人更改“文件和打印共享”。打开注册表编辑器，选择“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NetWork”主键，在该主键下新建DWORD类型的键值，键值名为“NoFileSharingControl”，键值设为“1”表示禁止这项功能，从而达到禁止更改“文件和打印共享”的目的；键值为“0”表示允许这项功能。这样在“网络邻居”的“属性”对话框中“文件和打印共享”就不复存在了。

3.把Guest账号禁用

有很多入侵都是通过这个账号进一步获得管理员密码或者权限的。如果不想把自己的计算机给别人当玩具，那还是禁止的好。打开控制面板，双击“用户和密码”，单击“高级”选项卡，再单击“高级”按钮，弹出本地用户和组窗口。在Guest账号上面点击右键，选择属性，在“常规”页中选中“账户已停用”。另外，将Administrator账号改名可以防止黑客知道自己的管理员账号，这会在很大程度上保证计算机安全。

4.禁止建立空连接

在默认的情况下，任何用户都可以通过空连接连上服务器，枚举账号并猜测密码。因此，我们必须禁止建立空连接。方法有以下两种：

方法一是修改注册表：打开注册表“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA”，将DWORD值“RestrictAnonymous”的键值改为“1”即可。

最后建议大家给自己的系统打上补丁，微软那些没完没了的补丁还是很有用的！

四、隐藏IP地址

黑客经常利用一些网络探测技术来查看我们的主机信息，主要目的就是得到网络中主机的IP地址。IP地址在网络安全上是一个很重要的概念，如果攻击者知道了你的IP地址，等于为他的攻击准备好了目标，他可以向这个IP发动各种进攻，如DoS(拒绝服务)攻击、Floop溢出攻击等。隐藏IP地址的主要方法是使用代理服务器。

与直接连接到Internet相比，使用代理服务器能保护上网用户的IP地址，从而保障上网安全。代理服务器的原理是在客户机（用户上网的计算机）和远程服务器（如用户想访问远端WWW服务器）之间架设一个“中转站”，当客户机向远程服务器提出服务要求后，代理服务器首先截取用户的请求，然后代理服务器将服务请求转交远程服务器，从而实现客户机和远程服务器之间的联系。很显然，使用代理服务器后，其它用户只能探测到代理服务器的IP地址而不是用户的IP地址，这就实现了隐藏用户IP地址的目的，保障了用户上网安全。提供免费代理服务器的网站有很多，你也可以自己用代理猎手等工具来查找。

五、关闭不必要的端口

黑客在入侵时常常会扫描你的计算机端口，如果安装了端口监视程序（比如Netwatch），该监视程序则会有警告提示。如果遇到这种入侵，可用工具软件关闭用不到的端口，比如，用“Norton Internet Security”关闭用来提供网页服务的80和443端口，其他一些不常用的端口也可关闭。

六、更换管理员帐户

Administrator帐户拥有最高的系统权限，一旦该帐户被人利用，后果不堪设想。黑客入侵的常用手段之一就是试图获得Administrator帐户的密码，所以我们要重新配置Administrator帐号。

首先是为Administrator帐户设置一个强大复杂的密码，然后我们重命名Administrator帐户，再创建一个没有管理员权限的Administrator帐户欺骗入侵者。这样一来，入侵者就很难搞清哪个帐户真正拥有管理员权限，也就在一定程度上减少了危险性。

七、杜绝Guest帐户的入侵

Guest帐户即所谓的来宾帐户，它可以访问计算机，但受到限制。不幸的是，Guest也为黑客入侵打开了方便之门！网上有很多文章中都介绍过如何利用Guest用户得到管理员权限的方法，所以要杜绝基于Guest帐户的系统入侵。

禁用或彻底删除Guest帐户是最好的办法，但在某些必须使用到Guest帐户的情况下，就需要通过其它途径来做好防御工作了。首先要给Guest设一个强壮的密码，然后详细设置Guest帐户对物理路径的访问权限。举例来说，如果你要防止Guest用户可以访问tool文件夹，可以右击该文件夹，在弹出菜单中选择“安全”标签，从中可看到可以访问此文件夹的所有用户。删除管理员之外的所有用户即可。或者在权限中为相应的用户设定权限，比方说只能“列出文件夹目录”和“读取”等，这样就安全多了。

八、安装必要的安全软件

我们还应在电脑中安装并使用必要的防黑软件，杀毒软件和防火墙都是必备的。在上网时打开它们，这样即便有黑客进攻我们的安全也是有保证的。

九、防范木马程序

木马程序会窃取所植入电脑中的有用信息，因此我们也要防止被黑客植入木马程序，常用的办法有：

● 在下载文件时先放到自己新建的文件夹里，再用杀毒软件来检测，起到提前预防的作用。

● 在“开始”→“程序”→“启动”或“开始”→“程序”→“Startup”选项里看是否有不明的运行项目，如果有，删除即可。

● 将注册表里 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run下的所有以“Run”为前缀的可疑程序全部删除即可。

十、不要回陌生人的邮件

有些黑客可能会冒充某些正规网站的名义，然后编个冠冕堂皇的理由寄一封信给你要求你输入上网的用户名称与密码，如果按下“确定”，你的帐号和密码就进了黑客的邮箱。所以不要随便回陌生人的邮件，即使他说得再动听再诱人也不上当。

做好IE的安全设置

ActiveX控件和 Applets有较强的功能，但也存在被人利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。所以要避免恶意网页的攻击只有禁止这些恶意代码的运行。IE对此提供了多种选择，具体设置步骤是：“工具”→“Internet选项”→“安全”→“自定义级别”，建议您将ActiveX控件与相关选项禁用。谨慎些总没有错！

另外，在IE的安全性设定中我们只能设定Internet、本地Intranet、受信任的站点、受限制的站点。不过，微软在这

里隐藏了“我的电脑”的安全性设定，通过修改注册表把该选项打开，可以使我们在对待ActiveX控件和 Applets时有更多的选择，并对本地电脑安全产生更大的影响。

下面是具体的方法：打开“开始”菜单中的“运行”，在弹出的“运行”对话框中输入Regedit.exe，打开注册表编辑器，点击前面的“+”号顺次展开到：
HKEY_CURRE-NT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\0，在右边窗口中找到DWORD值“Flags”，默认键值为十六进制的21(十进制33)，双击“Flags”，在弹出的对话框中将它的键值改为“1”即可，关闭注册表编辑器。无需重新启动电脑，重新打开IE，再次点击“工具→Internet选项→安全”标签，你就会看到多了一个“我的电脑”图标，在这里你可以设定它的安全等级。将它的安全等级设定高些，这样的防范更严密。