WINDOWS操作系统中如何防范IPC$入侵

吴成茂
(西昌学院,四川 西昌 615013)

【摘 要】IPC$是Windows操作系统中为了方便用户进行远程管理而使用的一项功能,然而在实际的应用中,IPC$并没有发挥太大的作用,反而为各类入侵提供了"后门"(Backdoor),在众多黑客的入侵手段中,通过IPC$入侵是目前比较常见的一种方式。

【关键词】IPC$;注册表;连接;端口
【中图分类号】TP316.7 【文献标识码】A 【文章编号】1673-1891(2010)02-0054-02

随着计算机网络应用范围的不断扩展,网络安全问题也变得越来越突出,特别是数据在存储和传输过程中,都有可能被盗用、暴露或篡改,这将给网络系统的应用带来一定的损失。IPC$是Windows中的一个重要模块,如"网上邻居"以及网络共享都是通过IPC$来实现的,黑客或者入侵者利用IPC$共享来实现入侵称为IPC$漏洞。IPC$连接分为IPC$空连接和带有一定权限IPC$连接,IPC$空连接没有任何权限,但是可以获取该主机的NETBIOS信息;而带有权限的IPC$连接则可以执行命令,并对文件进行复制、删除和修改等操作,从安全的角度来说,IPC$是一个存在安全隐患的因素。

1 什么是IPC$

IPC$是Internet Process Connection的缩写,也就是远程网络连接。它是WINDOWS NT/2000/XP/2003特有的一项功能。IPC后面的$是共享的意思,不过是隐藏的共享,微软系统中用"$"表示隐藏的共享。比如C$就是隐藏的共享C盘,也就是说C盘是共享的,但是C盘没有那个"托手"标志。IPC$是共享"命名管道"的资源,它是为了让进程间通信而开放的命名管道,可以通过验证用户名和密码获得相应的权限,在远程管理计算机和查看计算机的共享资源时使用。

2 IPC$入侵原理

IPC$入侵的最主要原理就是获取被入侵主机的密码,利用有权限的IPC$连接到主机并复制文件到主机上,然后运行木马程序或者执行命令来实现完全控制。如果系统默认共享全部打开,通过字典软件生成用户口令密码,再利用某些软件进行用户登录密码的暴力猜解,获取用户密码只是时间问题。因此IPC$安全是网络安全中一个不容忽视的问题,下面具体介绍IPC$的入侵过程:

2.1 启动"命令提示符"窗口

单击WINDOWS的"开始"菜单,执行"运行"命令,在出现的对话框中输入"CMD"命令并执行,即出现如图1所示的"命令提示符"窗口。

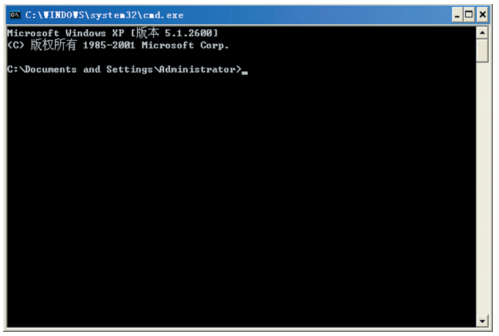

图1 "命令提示符"窗口

2.2 建立与远程主机

假设远程主机的IP地址为118.123.88.46的IPC$连接。命令为:

Net use \\118.123.88.46\IPC $ "123456"/user:"administrator"

连接成功后,将显示"命令成功完成"的提示信息,如图2所示:

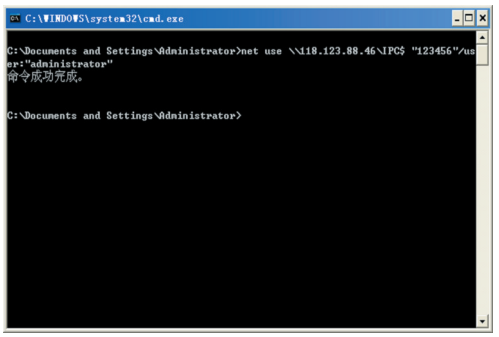

图2 建立IPC$远程连接

2.3 进行网络驱动器映射

在建立了与远程主机的IPC¥连接后,可以使用net use命令进行网络驱动器的映射操作。如将远程主机隐藏的E盘即E$映射为本地Y盘,命令如下:

Net use Y: \\118.123.88.46\E$

收稿日期:2010-05-09
作者简介:吴成茂(1976-),男,四川会东人,讲师,硕士,研究方向:计算机网络及网络安全。

连接成功后,将显示“命令成功完成”的提示信息,这时在本地计算机上打开“我的电脑”或“资源管理器”,就会发现多了一个“Y盘”,并可对该驱动器进行各类操作,包括创建文件、复制文件、删除文件等,与对本地磁盘的操作没有什么区别。

2.4 删除网络连接

当完成入侵后,入侵者为了不留下痕迹,一般会删除已创建的IPC$连接,具体命令为:

Net use */del

3 如何防范IPC$入侵

通过上面的分析可知,Windows(NT/2000/XP/2003)操作系统设置IPC$的初衷是为了方便管理员的管理,但该功能却被大量地应用于网络入侵,入侵者可以访问主机的共享资源、导出用户列表,并可以使用一些工具进行密码破解。因此防范IPC$入侵非常重要,常见的防御方法有:“禁止空连接”、“禁止默认共享”、“屏蔽139、445端口”、“停止Server服务”等。但有些方法也会使某些网络功能无法使用,如在服务器上停止服务器的“Server”服务,会使服务器的很多服务功能丧失,下面介绍一些实际操作中简单、切实可行的措施。

3.1 设置复杂的账号和密码

通过前面介绍的IPC$入侵过程,攻击者必须知道远程主机的账号和密码,才能进行IPC$连接,从而获取相关的权限,否则即便攻击者使用空用户名和空密码与远程主机进行连接,探测到远程主机的信息量也很少,并且不会拥有任何权限,无法执行相关的管理操作,因此设置较复杂的账号和密码是简单可行的措施。

3.2 安装和配置防火墙

防火墙是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障,是一种获取安全性方法的形象说法,它是一种计算机硬件和软件的结合,使Internet与Intranet之间建立起一个安全网关。入侵者必须首先穿越防火墙的安全防线,才能接触目标计算机,通过将防火墙配置成许多不同保护级别,使计算机中的信息等到很好的保护,对防范IPC$攻击也是一种重要的方案。

3.3 加密和备份重要数据

没有绝对安全的系统或方案,只要有网络存在,黑客总会编写或利用最新的攻击工具进行网络攻击。因此对重要的数据进行加密和备份,即使黑客侵入系统,窃取或破坏了这些数据,也不容易获取到数据的原文,并可将被破坏的数据进行还原。

4 结束语

微软公司的初衷都是为了方便管理员的管理,但好的初衷并不一定有好的收效,一些别有用心者会利用IPC$,访问共享资源,导出用户列表,并使用一些字典工具,进行密码探测,获得更高的权限,从而达到不可告人的目的,因此防范IPC$入侵是有必要的。

注释及参考文献:

[1]李馥娟.计算机网络实验教程[M].北京:清华大学出版社,2007.

[2]黑基网.IPC$入侵计算机系统浅析[EB/OL].http://www.hackbase.com/tech/2006-02-26/31374.html,2006-2-26/2010-5-10.

[3]曹炯清.Windows2000系统下IPC入侵和防范方法[J].计算机安全,2005,(6).

[4]李明柱,时亿杰.黑客攻击与安全防范技巧与实例[M].北京:北京航空航天大学出版社,2002.

How to Prevent IPC$ Intrusion in WINDOWS Operation System

WU Cheng-mao

(Xichang College, Xichang, Sichuan 615013)

Abstract: IPC$ is a function for users to make convenient remote management in Windows operation system. However, the IPC$ doesn't play an important role in practical use, but as a backdoor of various intrusions. Among many hacker's intrusion methods, the IPC$ is a common method of intrusion.

Key words: IPC$; Registry; Connection; Port