也说Windows XP系统安全巩固*

马 味,王 晔
(西昌学院 汽车与电子工程学院,四川 西昌 615000)

【摘 要】鉴于微软公司对Windows XP系统停止提供技术支持和漏洞修复,Windows XP用户既能使用“围篱笆”提供的服务,又可从帐户管理、帐户策略和禁用默认共享方面巩固系统。

【关键词】帐户管理;帐户策略;禁止默认共享;安全巩固
【中图分类号】TP316.89 【文献标志码】A 【文章编号】1673-1891(2015)02-0068-04
DOI:10.16104/j.cnki.xccxb.2015.02.023

引言

据CNZZ调查统计,至2013年10月,我国的Windows XP用户比例达59%。《中国企业杀毒软件产品市场调研报告》显示,Windows XP系统在中国企业市场占有高达43%的份额,甚至在部分政府单位和大型企业中Windows XP系统的应用比例超过了60%[1]。这两大调查证明中国Windows XP用户数量巨大。可是,2014年4月8日,微软公司停止提供Windows XP系统技术支持与安全漏洞修复,很多Windows XP用户由于自身或其他原因,不能及时升级到Windows 7或Windows 8等更新更安全的系统。确保XP系统的安全将是一个非常重要的问题。

大多数Windows XP用户会启动Windows自带的防火墙,安装杀毒软件并定期对系统杀毒、升级病毒库,安装安全卫士并定期对电脑进行体检,还有利用“围篱笆”提供的“系统升级援助”、“XP系统安全主动防御”、“XP救援服务站”、“XP用户专版安全软件”等的一系列安全服务。笔者认为还可从帐户管理、禁用默认共享、帐户策略方面巩固Windows XP系统的安全。

1 帐号管理

用户在命令提示符界面输入net user以后可看到用户列表,包括Administrator和Guest这两个帐户。它们是系统安装完以后自动创建的。如果用户没有对此做相应设置的话,将存在一定的安全隐患。

1.1 Administrator设置密码及更名

Administrator帐户是系统自动创建并且密码为空的超级管理员帐户,权限非常大,不能删除或者禁用。如果用户没有进行相关的设置,非法用户通过它很容易进入用户电脑,轻者窃取或者删除重要资料,重者让系统瘫痪。所以,首先要对Administrator帐户设置密码。这一密码最好采用字母、数字和符号的组合,长度最好大于等于8个字符。这样的密码是抗攻击的最好密码,可通过控制面板里面的[用户帐户]窗口设置Administrator密码。其次,最好更名Administrator帐户,不能使用admin这样的名字,要尽量将Administrator伪装为普通用户,如Guest 1或者Guestone。详细来讲,Administrator帐户更名的操作顺序为:[控制面板]→[管理工具]→[计算机管理]→[本地用户和组]→[用户],再在右边窗格中右键选中Administrator,选择[重命名]完成[2]。如图1所示。

图1 计算机管理窗口用户

1.2 Guest帐户停用

Guest帐户也是系统安装完毕以后默认建立的帐户。该帐户的权限最低,以便浏览者查看计算机上的一些资源。黑客可将该帐户的权限提升到管理员权限,从而给用户计算机带来危害。因此,停用Guest帐户可加强系统的安全。在图1的[计算机管理]窗口里面,右击Guest帐户后选择[属性],在[Guest属性]窗户里面的[常规]选项卡中勾选[帐户已停用],点击[应用]和[确定]按钮即完成设置。如图2所示。

收稿日期:2015-03-10
*基金项目:西昌学院研究生项目“VBA在Excel中的应用研究”(项目编号:XY09-ZA18)。
作者简介:马味(1981-),女,回族,四川西昌人,讲师,软件工程硕士,研究方向:计算机基础与系统安全。

图2　Guest属性窗口

1.3 陷阱帐户

陷阱帐户是创建一Guest组,名字为"Administrator"的本地帐户。它同时还有一超过10位的超级复杂的密码,这样可花费那些企图入侵者很多时间,又可借此发现入侵者的企图。详细步骤为先创建新用户,再将该用户添加到Guest组。创建新用户的步骤为:[计算机管理]窗口中右击右侧窗格的空白地方,选择[新用户],打开[新用户]对话框,输入用户名及密码,再选择[创建]按钮。将该用户添加到Guest组的步骤为:在图2所示的Guest属性窗口的[隶属于]选项卡里进行添加操作。

2 禁用默认共享

默认共享是在计算机系统安装后自动开启的管理共享,管理员常用它来管理远程计算机。这也给黑客带来了可乘之机。黑客通过这些共享磁盘分区,随意进入用户计算机,给用户带来不安全因素。因此,禁用默认共享可彻底消除安全隐患[3,4]。

2.1 查看默认共享

在Windows XP里面,默认开启的共享为所有分区磁盘及"admin$"、"ipc$"。这些共享都有"$"标志,表示共享状态是隐藏的。[网上邻居]中找不到这种隐藏的默认分区,用户只能在[运行]对话框中输入"\\计算机名或IP地址\盘符$"对这些默认共享进行访问,或者在浏览器的地址栏中输入"file:// 计算机名或IP地址/盘符$"来访问。查看默认共享资源可通过以下两种方法来实现。

● 使用net share命令

详细步骤为:执行[开始]→[运行],在运行对话框中输入"cmd",选择[确定]按钮。打开命令提示符窗口并输入"net share"查看所有开启的默认共享资源。

● 使用[计算机管理]窗口查看

右击[我的电脑]→[管理]→[计算机管理],在计算机管理窗口中展开[共享文件夹]节点,并单击[共享]选项。在右侧窗格中就能看见默认共享资源。如图3所示。

图3　计算机管理窗口的共享

2.2 停止默认共享

停止默认共享可使用net share命令、计算机管理窗口、关闭Server服务、修改注册表和卸载[文件和打印机共享]进行设置。其中net share命令和计算机管理窗口只能暂时关闭默认共享。关闭Server服务和修改注册表可永久关闭共享。卸载"文件和打印机共享"后,系统不能再给任何人提供共享功能,一般不推荐使用。下面依次介绍。

● net share命令

net share命令关闭默认共享与net share查看默认共享操作基本相同,在命令提示符窗口输入"net share 盘符$/ delete"命令,按回车键删除指定的默认共享。如输入"net share C$/ delete"(delete前必须有空格)并按回车键,显示C$已经删除的信息。使用同样的方法可删除D$、E$、Admin$、IPC$等默认共享。

另外,还能使用批处理命令在开机时自动关闭全部的默认共享。详细步骤为:

打开记事本程序,输入图4所示的命令,将该文件另存为批处理文件(即文件扩展名为.bat),将该文件拖到启动子菜单下。这样每次启动计算机时,就会运行该批处理文件,关闭所有的默认共享。也可双击.bat文件或在命令提示符下运行.bat文件都可关闭默认共享。用户还可根据需要选择关闭默认共享,只要打开.bat文件即能进行修改。

图4 批处理命令编写

● 计算机管理窗口

使用计算机管理窗口查看默认共享的界面中，右击选中的默认共享，选择[操作]→[停止共享]，弹出[共享文件夹]提示框，选择[是]按钮完成选定默认共享的关闭。

● 关闭Server服务

详细步骤为：

[开始]→[运行]，在[运行]对话框中输入 services.msc，单击 [确定] 按钮打开服务窗口。或者依次选择[控制面版]→[管理工具]→[服务]打开服务窗口，在右侧窗格中双击 server，打开 server 属性（本地计算机）窗口，将启动类型改为[已禁用]，单击[停止]按钮，再单击[应用]、[确定]按钮。如图5所示。

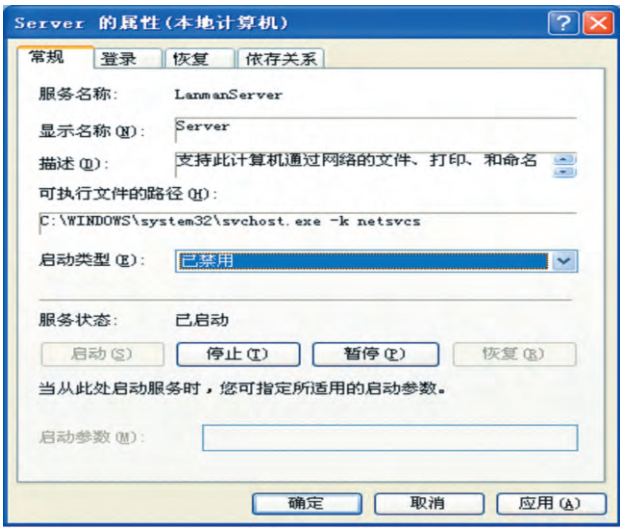

图5 Server的属性窗口

● 修改注册表

利用注册表编辑器可将默认共享永久关闭。详细实现是通过创建DWROD键值，将它的值设为0。详细步骤为：

在[运行]中输入 regedit 命令打开注册表编辑器，选择主键 HEKY_LOCAL_MACHINE，在该主键下选择子键：

SYSTEM\CurrentControlSet\Set\Services\Lanman Serve\AutotunedParameters，右击右侧窗格的空白地方，[新建]→[DWROD值]菜单项，创建名为AutoShareServer的DWROD值，并将其赋值为“0”。如图6所示。

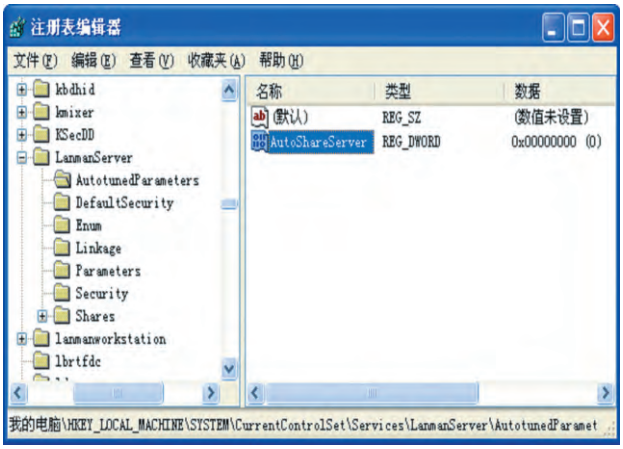

图6 创建AutoShareServer键值

● 卸载“文件和打印机共享”

在Windows XP系统中，所有共享功能都是通过“文件和打印机共享”服务提供的。若将其卸载，默认共享就被彻底关闭，同时计算机也就不存在任何共享功能。所以，一般不推荐使用该方法关闭默认共享。卸载“文件和打印机共享”是通过本地连接属性对话框来实现的，选中[Microsoft 网络的文件与打印机共享]→[卸载]按钮，按默认步骤执行。

3 帐户策略设置

帐户策略有密码策略和账户锁定策略两种。其中，通过密码策略的设置可加强密码的破解难度。帐户锁定策略可有效地避免自动猜测工具的攻击，同时也可打击手动尝试者[3,4]。

3.1 密码策略

通过执行[开始]→[管理工具]→[本地安全策略]→[帐户策略]→[密码策略]，查看所有的密码策略选项。常用的选项为[密码必须符合复杂性要求]、[密码长度最小值]、[密码最长存留期]和[密码最短存留期]。其中，[密码必须符合复杂性要求]是指密码中必须包含字母、数字、特殊字符等，强制用户必须使用经过复杂设置的密码。[密码长度最小值]确定用户的帐户密码可包含的最少字符数，推荐8位及以上字符。[密码最长存留期]确定用户更换密码以前可使用该密码的天数，推荐30～90天之间。[密码最短存留期]确定用户在更改密码以前必须使用该密码的天数，可设置一介于1和998天之间的值，或者将天数设置为0，能立即更改密码。这些选项的启用总是右击相应选报后选择[属性]完成。

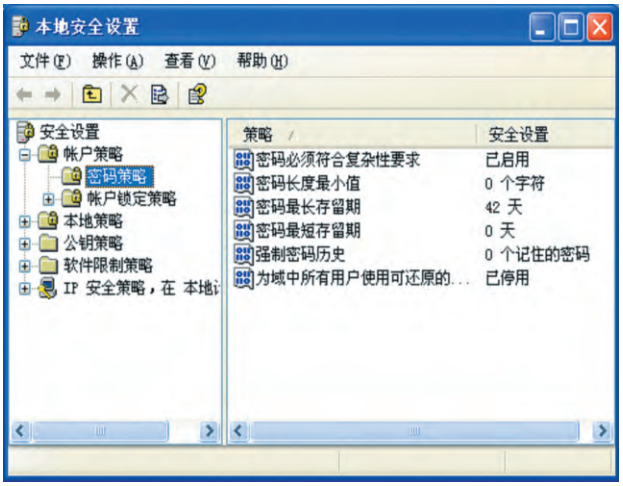

图7　密码策略窗口

3.2 账户锁定策略

帐户锁定是指当帐户受到密码词典或暴力破解等方式的在线自动登录工具攻击时,将此帐户进行锁定,使其在一段时间内不能再次使用的策略。帐户策略主要由帐户锁定阈值、账户锁定时间和复位账户锁定计数器组成。帐户锁定阈值确定用户帐户被锁定登录的失败次数,建议值为3~5。账户锁定时间确定帐户在自动解锁前保持锁定状态的分钟数,有效范围为0~99999分钟之间。复位账户锁定计数器确定在登录尝试失败计数器重置为0以前,尝试登录失败之后所需的时间[5]。如图8所示。

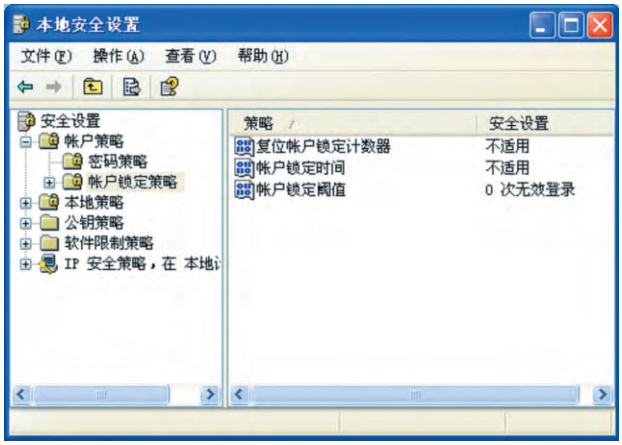

图8　帐户锁定策略窗口

通常为了保护用户帐户安全,推荐的帐户策略应包括以下内容:

启动[密码必须符合复杂性要求],推荐密码长度最小值为8个字符或更高,账户锁定阈值为3或者更高,复位帐户锁定计数器设置为30分钟以后。

4　结语

微软公司自2014年4月8日停止了提供Windows XP系统技术支持与安全漏洞修复,笔者建议数量巨大的Windows XP系统用户通过帐户管理、禁用默认共享和帐户策略的设置加固计算机系统安全。Windows XP系统用户最好选择新系统是上策。

注释及参考文献:

[1]http://www.docin.com/p-837599565.html.
[2]石志国.计算机网络安全教程[M].北京:清华大学出版社,2011: 227-235.
[3]导向工作室.24小时学会黑客功放[M].北京:人民邮电出版社,2011: 165-173.
[4]武新华.黑客攻防实战从入门到精通第2版[M].北京:科学出版社,2011:25-28.
[5]陈中平.网络安全[M] .北京:清华大学出版社,2011: 113-116,127-132.

We to Reinforce the Security of Windows XP System

MA Wei, WANG Ye
(School of Automotive and Electronic Engineering, Xichang College, Xichang, Sichuan 615013)

Abstract: Because Microsoft ceased providing technical support and bug fixes for Windows XP system, the users of Windows XP system not only can use the services of "firm fence" providing, but also should reinforce Windows XP system from accounts management, forbid default shared, and accounts strategies.

Key words: accounts management; accounts strategies; forbid default shared; reinforce security