

安全设置WinXP操作系统的技巧Microsoft认证考试 PDF转换
可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/643/2021_2022__E5_AE_89_E5_85_A8_E8_AE_BE_E7_c100_643902.htm Windows XP以其稳定性、强大的个人和网络功能为大家所推崇，而它的“NT内核”，让我们不得不加强安全防护。1. 常规的安全防护所谓“常规的安全防护”即施行同Windows 98一样的安装防病毒软件、升级系统、禁止Ping三种安全方式。要强调的是Windows XP和它的前辈Windows 2000一样，漏洞层出不穷，对于系统的升级不能像对Windows 98般马虎，除了要安装Microsoft针对“冲击波”的漏洞补丁外，建议将Windows XP升级为最新的Service Pack 1(升级后会提高资源占有，不过安全性、稳定性有所提高)。2. 禁止远程协助，屏蔽闲置的端口在Windows XP上有一项名为“远程协助”的功能，它允许用户在使用计算机发生困难时，向MSN上的好友发出远程协助邀请，来帮助自己解决问题。而这个“远程协助”功能正是“冲击波”病毒所要攻击的RPC(Remote Procedure Call)服务在Windows XP上的表现形式。建议用户不要使用该功能，使用前也应该安装Microsoft提供的RPC漏洞工具和“冲击波”免疫程序。禁止“远程协助”的方法是：打开系统属性对话框(右键“我的电脑”、“属性”)，在“远程”项里去掉“允许从这台计算机发送远程协助邀请”前面的“”。使用系统自带的“TCP/IP筛选服务”就能够限制端口。方法如下：在“网络连接”上单击右键，选择“属性”，打开“网络连接属性”对话框，在“常规”项里选中里面的“Internet协议(TCP/IP)”然后单击下面的[属性]按钮，在“Internet协

议(TCP/IP)属性”窗口里，单击下面的[高级]按钮，在弹出的“高级TCP/IP设置”窗口里选择“选项”项，再单击下面的[属性]按钮，最后弹出“TCP/IP筛选”窗口，通过窗口里的“只允许”单选框，分别添加“TCP”、“UDP”、“IP”等网络协议允许的端口，未提供各种服务的情况，可以屏蔽掉所有的端口。这是最佳的安全防范形式。

3. 禁止终端服务远程控制

“终端服务”是Windows XP在Windows 2000系统(Windows 2000利用此服务实现远程的服务器托管)上遗留下来的一种服务形式。用户利用终端可以实现远程控制。“终端服务”和“远程协助”是有一定区别的，虽然都实现的是远程控制，终端服务更注重用户的登录管理权限，它的每次连接都需要当前系统的一个具体登录ID，且相互隔离，“终端服务”独立于当前计算机用户的邀请，可以独立、自由登录远程计算机。在Windows XP系统下，“终端服务”是被默认打开的，(Windows 2000系统需要安装相应的组件，才可以开启和使用终端服务)也就是说，如果有人知道你计算机上的一个用户登录ID，并且知道计算机的IP，它就可以完全控制你的计算机。在Windows XP系统里关闭“终端服务”的方法如下：右键选择“我的电脑”、“属性”，选择“远程”项，去掉“允许用户远程连接到这台计算机”前面的“”即可。

4. 关闭Messenger服务

Messenger服务是Microsoft集成在Windows XP系统里的一个通讯组件，它默认情况下也是被打开的。利用它发送信息时，只要知道对方的IP，然后输入文字，对方的桌面上就会弹出相应的文字信息窗口，且在未关闭掉Messenger服务的情况下强行接受。很多用户不知道怎么关闭它，而饱受信息的骚扰。其实方法很简单，进入“控

制面板”，选择“管理工具”，启动里面的“服务”项，然后在Messenger项上单击右键，选择“停止”即可。

5. 防范IPC默认共享

Windows XP在默认安装后允许任何用户通过空用户连接(IPC\$)得到系统所有账号和共享列表，这本来是为了方便局域网用户共享资源和文件的，但是任何一个远程用户都可以利用这个空的连接得到你的用户列表。黑客就利用这项功能，查找系统的用户列表，并使用一些字典工具，对系统进行攻击。这就是网上较流行的IPC攻击。要防范IPC攻击就应该从系统的默认配置下手，可以通过修改注册表弥补漏洞：

第一步：将HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA的RestrictAnonymous项设置为“1”，就能禁止空用户连接。

第二步：打开注册表的HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters项。对于服务器，添加键值“AutoShareServer”，类型为“REG_DWORD”，值为“0”。于客户机，添加键值“AutoShareWks”，类型为“REG_DWORD”，值为“0”。

6. 合理管理Administrator

Windows 2000/XP系统，系统安装后都会默认创建一个Administrator用户，它拥有计算机的最高管理权限。而有的用户在安装时，根本没有给Administrator用户设置密码。黑客就利用这一点，使用高级用户登录对方计算机。因此，个人用户应该妥善保管“Administrator”用户信息，Windows 2000登录时，要求输入Administrator用户的登录密码，而Windows XP在正常启动后，是看不到Administrator用户的，建议使用Windows XP的用户进入安全模式，再在“控制面

板”的“用户账户”项里为Administrator用户添加密码，或者将其删除掉，以免留下隐患。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com