微软认证辅导:Windows系统本身的安全设置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_ti2020/607/2021_2022__E5_BE_AE_E8_BD_AF_E8_AE_A4_E8_c100_607702.htm 一、系统与磁盘格式选择 1、不要使用Ghost版的Windows XP系统 在选用操作系统时，最好不要选择Ghost版的Windows XP系统，因为使用此系统版本的用户，默认情况下会自动开启远程终端服务，并且还会存在一个弱口令形式的new账号，两者很容易被黑客利用，从而导致最后计算机被别有用心的人入侵。当然如果只有Ghost版的Windows XP系统安装盘也没关系，不过要注意的是请在系统安装完成后，依次单击“ 开始 ”→“ 运行 ”选项，在打开的“ 运行 ”对话框内，输入services.msc命令回车，此时就会启动“ 服务 ”列表对话框。从中找到terminal services服务项后，将其属性更改为“ 已禁用 ”选项确定即可。 2、磁盘选用NTFS格式 NTFS分区格式是随着Windows NT操作系统而产生的，并随着Windows NT4跨入主力分区格式的行列，它的优点是安全性和稳定性极其出色，在使用中不易产生产生文件碎片，NTFS分区对用户权限作出了非常严格的限制，每个用户都只能按着系统赋予的权限进行操作，任何试图越权的操作都将被系统禁止，同时它还提供了容错结构日志，可以将用户的操作全部记录下来，从而保护了系统的安全。NTFS文件系统还具有其他的优点，如：对于超过4GB以上的硬盘，使用NTFS分区，可以减少磁盘碎片的数量，大大提高硬盘的利用率。NTFS可以支持的文件大小可以达到64GB，远远大于FAT32下的4GB，支持长文件名等等。 3、收集罪证缉拿黑客 众所周知，审核登录是本地策略里的一个安全功能

，所以要想利用审核登录制止黑客的非法入侵。这里首先应当启动本地安全策略，具体操作如下：依次单击“ 开始 ”→“ 运行 ”选项，在打开的“ 运行 ”对话框内，输入“ control admintools ”命令回车，在所显示的“ 管理工具 ”页面内，双击“ 本地策略 ”标签项，此时就会弹出“ 本地安全设置 ”对话框。在其左侧展开“ 本地策略 ”选项，单击“ 审核策略 ”标签，而后在双击右侧“ 审核登录事件 ”选项，将“ 审核这些操作中 ”的“ 成功 ”、“ 失败 ”都选上后，在以相同的方法把“ 审核账号管理 ”、“ 审核账号登录事件 ”，以及“ 审核目录服务访问 ”都设置好后，系统会把远程入侵者的信息记录到日志，以便于我们能够“ 顺藤摸瓜 ”的抓住黑客。至于如何查找记录非法入侵者信息，我们可以通过在“ 运行 ”对话框内，输入eventvwr.msc命令将“ 事件查看器 ”打开，即可进行查看。 二、系统权限设置 1、对磁盘进行权限设置 要想对磁盘进行权限设置，前提条件你的系统必须是Win2k以上的操作系统，但是Windows XP家庭版用户除外，并且其磁盘驱动器都均为NTFS文件形式，以上两者缺一不可。然后才可以右击你想要设置的盘符驱动器，选择“ 属性 ”选项，添加 adminitrator和system确定后，再选择everyone用户将其删除，单击“ 高级 ”勾选上里面“ 重置所有子对象的权限并允许传播可继承权限 ”即可。 2、某些文件的权限设置 如果你要想对某些单个文件权限进行设置，我们可以通过在命令行下的cacls命令，对其文件进行权限设置。这里不排除很多人都对cacls命令的使用比较陌生，可以在CMD命令行下，输入cacls /?命令，就可在其CMD命令行下的区域显示出该命令的详细用法。这里以这里就拿123.txt文件为例，在命令行下输

入cacls 123.txt /e /g administrator:f命令回车后，就可对其文件进行处理。等到光标另起一行后，输入type 23.txt试探一下情况，此时就会出现拒绝访问的提示信息。另外把该文件移动到系统盘的根目录下，在一定程度上也可以防止木马对其的加载。 3、注册表启动项的权限设置 为了防止恶意程序在注册表的启动项内，修改一些重要的设置，我们可以给其启动项，做一下相关的权限设置，就可避免此类恶意情况出现。这里打开“ 运行 ”对话框，输入regedt32命令回车后，在弹出的“ 注册表 ”对话框内，依次展开左侧主件到HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun下，右击该键值选择“ 权限 ”选项。然后单击“ 高级 ”，将“ 从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目(I) ”前的勾去掉，然后单击“ 确定 ”按钮，将 administrator和system账号以外的用户删除。操作完毕后，勾选上“ 从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目(I) ”即可。 三、系统服务的安全操作 要想查看服务列表，请在桌面内依次单击“ 开始→“ 运行 ”选项，在打开的对话框里，输入services.msc命令回车后，就可打开“ 系统服务列表 ”对话框窗口。 其服务列表右侧所罗列出来的是当前系统所有安装的程序服务，如果你对这里某个服务不太了解，可以通过双击该服务栏，在弹出的“ 属性 ”对话框内，就可观看到其服务的描述情况。当然有些时候，你可能会碰到描述情况为空，或者其描述与名称“ 驴头不对马嘴 ”，那么它们就很有可能就是木马所加载到系统的服务，笔者建议你最好是将这样的可疑服务马上关闭，以避免不必要的麻烦。 1、禁

用Alter/messeng信使服务 基于Alter/messeng信使服务，虽然可以使管理员向网络中的其他用户发送信息，但是QQ和MSN聊天软件的出现，足以代替其服务的所有功能，而且两个聊天软件在通讯方面非常强悍，要比基于服务发送信息强的多。另外恶意人可以利用该服务，使用net send向网络中的用户发垃圾信息，能够影响到用户正常的上网。所以为此你最好在列表服务对话框内，双击messeng信使服务，在弹出的属性对话框内，将其信使服务的启动类型，选择为“ 已禁用 ”选项，就可将其服务关闭。 2、禁用clipbook服务 clipbook服务的开启，可以使管理员能够轻松查看本地剪贴板里的内容，但是该服务被黑客所利用，同样也会为其提供便捷的查看剪贴板。如果此时是一个喜欢将密码复制到剪贴板，再将进行粘贴到相关位置的人，可想而知被人利用的后果，将是不堪设想的。 因此这里同样在服务“ 列表 ”对话框内，找到且双击clipbook服务名称，在弹出的“ 相关属性 ”对话框内，将启动项列表选择为已禁用，就可将其服务进行关闭。 3、禁用Remote Registry服务 虽然开放Remote Registry服务，可以让管理员远程操控其他计算机的注册表，但是殊不知它也会给我们带来潜在的安全隐患。比如对方获取了我们本地计算机的账号及密码，并且IPC$空连接服务也是启动，那么黑客就可以基于此服务在启动项里加载上一个自启动的恶意程序，可想而知你的计算机以后就要听命于他。所以 Remote Registry服务也要将其禁用，其操作方法同上便可。 4、关闭Task Scheduler服务 一般远程入侵者，在通过IPC$空命令连接到被害主机后，为了便于接下来的远程操控，都会将其远程控制木马上传到受害主机内，然后在使用At命令激活刚才所上传

的木马，使其发挥作用。而其使用At命令是基于Task Scheduler计划服务运行的，所以为了防止黑客在自己的主机上激活木马，请将其Task Scheduler服务关闭掉，这样即使以后你的机器真被黑客上传了木马，它也无法激活并运行其木马。 5、禁用Terminal services服务 Terminal services服务，也就是大家经常叫远程终端，此服务的开放可以允许多个用户连接并控制一台机器，并且在远程计算机上所显示的桌面和应用程序，可以非常直观的进行观看、操控。如果黑客利用Terminal services服务登录主机，后果自然是不言而喻的，所以为了对其服务防患于未然。这里同样在服务列表里，打开“ Terminal services服务 ”的属性对话框，将其启动类型更改为“ 已禁用 ”状态后，单击“ 确定 ”按钮使其生效。然后右击“ 我的电脑 ”图标，选择“ 属性 ”选项，在弹出的“ 系统属性 ”对话框内，切入至上方“ 远程 ”标签，将里面“ 允许从这台计算机发送远程协助邀请 ”的复选框勾去掉即可。四、利用好Windows XP自带的安全中心，可以有效防止外来攻击 虽然微软漏洞很多，但是Windows XP自带的安全中心，也算是广大用户防御攻击一个“ 安慰 ”。该安全中心不仅为用户提供了防火墙功能，而且就连病毒保护软件、自动更新系统漏洞的防御措施，也都内置在其安全中心内了。如果此时你要进入到安全中心，只要在桌面依次单击“ 开始→控制面板→安全中心 ”选项，就可打开“ 安全中心 ”对话框进入。 要想阻止其他网站所弹出的窗口，这里我们单击下面的“ Internet选项 ”标签，在弹出的“ Internet属性 ”对话框内，切入至上方“ 隐私 ”标签处，此时你会发现下面会多出一个弹出“ 窗口阻止 ”程序栏，然后我们单击其栏目里的“ 设置

” 按钮，在弹出的 “ 阻止程序设置 ” 对话框内，将要允许的网站地址输入到文本框内，这样你就只能接受一些自己设置的正规网站弹出的窗口。另外该安全中心还提供了防火墙功能，你只要在其下方单击 “ Windows 防火墙 ” 标签，就可弹出 “ Windows 防火墙 ” 对话框窗口，然后从中选中里面 “ 启用 ” 单选框项，单击 “ 确定 ” 按钮，便可发挥内置的防火墙抵御外界攻击的作用。除此之外如果你不愿意去微软的网站去下载补丁，可以单击下方 “ 自动更新 ” 标签，在弹出的 “ 自动更新 ” 对话框内，设置好更新时间，其系统就会在你所指定的时间，自动帮你更新系统下载安全补丁了。