 为了提高工作效率，相信很多网络管理员都喜欢使用远程控制方式来管理网络，这种方式允许管理员在局域网的任何位置处对重要主机进行管理、维护，确保网络能够始终高效、稳定运行。不过，在享受远程控制带给自己便利的同时，我们也容易遭遇远程入侵安全威胁.为了让远程网络控制的安全更上一层楼，本文现在就为各位朋友贡献几则安全防护技巧，希望下面内容能给大家带来启发! 使用陌生端口进行远程控制 为了让网络控制效率更高一些，很多人总喜欢借助远程登录功能来对远程主机进行控制与管理.可是，在利用Telnet命令进行远程登录控制操作时，我们往往都是使用默认的“ 23 ”端口与远程主机进行连接的，而这个默认的端口号码很多时候会被非法攻击者利用，从而可能会给远程控制操作带来安全威胁。为了让远程控制操作更加安全，我们可以自己动手，将默认的“ 23 ”端口修改成陌生的端口号码，日后非法攻击者由于不知道远程控制端口号码，那么他们自然也就不能对远程控制操作带来什么安全威胁了，下面是快速修改远程登录端口号码的具体设置步骤： 首先以系统管理员权限进入目标远程主机系统，打开该系统桌面中的“ 开始 ”菜单，从中点选“ 运行 ”命令，在弹出的系统运行对话框中，输入字符串命令“ cmd ”，单击“ 确定 ”按钮后，进入对应系统的DOS命令行工作界面. 其次在该界面的命令行提示符下，输入“ tlntadmn config port=989 ”字符串命令，其中“ 989 ”为任意指定的一

个远程登录端口号码，该号码不能与其他已开通端口号码相同，单击回车键后，对应系统的远程控制端口号码就从默认的“ 23 ”变成“ 989 ”了。 成功修改好远程控制端口号码后，我们必须确保该陌生的端口号码不能让其他人知道.此外，我们日后需要通过telnet命令与目标主机系统建立远程控制连接时，必须使用类似“ telnet host port ”这样的命令方式，其中host为远程主机的名称或IP地址，port为新的控制端口号码.例如，要远程登录到10.176.6.1主机时，我们可以在DOS命令行状态执行“ telnet 10.176.6.1 989 ”字符串命令就可以了。 使用高级防火墙保护远程连接 除了利用telnet功能对局域网中的重要主机进行远程控制外，网络管理员还可能会利用Windows系统自带的远程桌面连接功能来对重要主机进行网络控制。为了防止普通用户利用远程桌面连接功能对局域网中的重要主机进行非法攻击，我们可以想办法来保护合法用户的远程桌面连接，禁止非法用户与重要主机创建远程桌面连接.在Windows Vista以上版本的系统环境中，我们可以利用系统自带的高级安全防火墙功能，来保护合法用户的远程桌面连接，下面就是具体的设置步骤： 首先打开Windows Vista系统的“ 开始 ”菜单，从中点选“ 运行 ”命令，在弹出的系统运行对话框中，执行字符串命令“ mmc ”，进入对应系统的控制台界面.单击该界面中的“ 文件 ”菜单项，从下拉菜单中点选“ 添加/删除管理单元 ”选项，选中“ 可用管理单元 ”列表框中的“ 高级安全Windows防火墙 ”项目，同时单击“ 添加 ” 按钮，再单击“ 确定 ”按钮. 其次选中Windows Vista系统控制台界面左侧位置处的“ 高级安全Windows防火墙 ”项目，打开高级安全防火墙主界面，单击其中的“ 入站

规则”功能选项，同时点击该选项下面的“新规则”按钮，弹出新建入站规则向导窗口.考虑到远程桌面连接需要使用3389网络端口，所以当新建入站规则向导窗口提示我们建立什么类型的规则时，我们应该毫不犹豫地将“端口”选项选中，以便创建控制远程桌面连接端口的规则. 单击“下一步”按钮，依照提示选中“TCP协议”，同时将“特定本地端口”项目也选中，之后在对应文本框中正确填写好远程桌面连接端口号码“3389”，在其后界面中选中“只允许安全连接”功能选项，以便只能局域网中特定的计算机进行远程桌面连接.接下来系统屏幕会弹出设置页面，将其中的“只允许来自下列计算机的连接”项目选中，同时单击“添加”按钮，打开计算机选择对话框，从中将我们认为值得信任的合法计算机名称或IP地址选中并加入进来. 下面再将“域”、“专用”、“公用”等选项全部选中，同时为当前创建的安全规则设置一个合适的规则名称，再点击“完成”按钮保存好入站规则的设置操作。如此一来，日后我们只能从局域网中的特定计算机中利用远程桌面连接功能，来对重要主机进行远程控制操作，其他计算机用户在尝试与局域网中的重要主机建立远程桌面连接时，会受到对应系统高级安全防火墙的严格限制。 设置权限禁止随意修改控制规则 前面我们也知道，在Windows Vista以上版本的系统环境中，我们可以利用高级安全防火墙功能自由定义各种各样的安全规则，来确保网络控制的绝对安全。不过，有一些高明的黑客为了穿越安全规则的限制，他们有时会想方设法修改高级安全防火墙的控制规则，以便取得非法控制权限.有鉴于此，我们可以尝试按照下面的设置操作，来禁止普通用户随意修改高级安全防火墙

的各种控制规则：首先在Windows Vista系统桌面中依次点击“开始”、“运行”选项，在系统运行框中输入“regedit”字符串命令，单击“确定”按钮后进入对应本地系统的注册表编辑界面.展开该界面左侧位置处的HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules分支选项，从该注册表分支下面我们看到许多防火墙的安全规则都保存在其中. 很显然，要是允许任何普通用户随意访问FirewallRules分支选项下面的内容时，那么防火墙的安全规则可能会受到修改破坏，为此我们要想办法禁止 Everyone帐号对FirewallRules分支内容进行访问。要做到这一点其实很简单，我们只要将鼠标定位于FirewallRules分支选项上，再依次单击注册表编辑窗口菜单栏中的“编辑”/“权限”命令，在弹出的目标分支权限设置窗口中单击“添加”按钮，进入用户帐号选择设置框，将“Everyone”帐号选中并将导入进来. 接下来返回到用户帐号列表框，将刚刚添加进来的“Everyone”帐号选中，同时将对应该帐号的“完全控制”权限设置为“拒绝”，再单击“确定”按钮保存好上述设置操作，这样的话非法攻击者日后就无法随意修改Windows Vista系统的安全规则了，那么日后的网络控制操作或许就能受到高级安全防火墙的保护了。 授权特定用进行远程桌面连接 一般来说，属于Administrator组的用户在默认状态下都能对局域网中的重要主机进行远程桌面连接，但是在实际进行远程控制的过程中，我们有时只允许一个特定用户对重要主机进行远程桌面连接，其他用户哪怕是系统管理员也不能随便对重要主机进行远程控制，这样可以保证重要主机的绝对安全。遇到这种

情形时，我们可以对远程桌面连接权限进行设置，让其只赋予自己信任的特定用户，下面就是具体的设置步骤：首先以系统管理员权限进入局域网目标重要主机系统，用鼠标右键单击该系统桌面中的“ 我的电脑 ”图标，从弹出的快捷菜单中执行“ 属性 ”命令，打开对应系统的属性设置窗口. 其次单击该设置窗口中的“ 远程 ”选项卡，在对应选项设置页面的“ 远程桌面 ”位置处，选中“ 允许用户远程连接到这台计算机 ”选项，同时单击对应选项下面的“ 选择远程用户 ”按钮，打开设置对话框，在这里我们发现凡是隶属于Administrator组的用户在默认状态下都能通过远程桌面连接功能对本地系统进行远程控制. 为了保证远程控制的绝对安全性，我们应该先将默认授权的Administrator组帐号选中，同时单击“ 删除 ”按钮，取消Administrator组帐号的远程桌面连接权限.之后，单击“ 添加 ”按钮，从弹出的用户账号选择对话框中，将我们认为值得信任的特定账号名称选中并添加进来，再单击“ 确定 ”按钮执行设置保存操作，这么一来日后只有指定的用户才能通过远程桌面连接功能对本地系统进行远程控制，其他任何用户包括网络管理员都无法对其进行远程控制操作，那么网络控制的安全性也就能得到有效保证了。 设置策略谨防远程窃取权限账号 不少技术高明的非法攻击者常常会通过登录远程目标系统的SID标识，来偷窃具有系统管理员权限的账号名称，日后再尝试通过暴力破解的方法来获取对应帐号的密码，如此一来他们就有可能获得整个系统的远程控制权限，很显然，要是远程目标系统的系统管理员权限帐号名称被他人偷窃得到的话，那么远程主机系统的安全性就可能会受到威胁了。为了谨防非法攻击者偷窃远程主机系统的系统

管理员帐号名称，我们可以按照下面的方法修改远程主机系统的组策略参数： 首先以系统管理员权限帐号进入远程主机系统，打开该系统桌面中的“ 开始 ”菜单，从中单击“ 运行 ”命令，打开对应系统的运行文本框，在其中输入“ gpedit.msc ”字符串命令，进入远程主机系统的组策略控制台界面. 其次展开该控制台界面左侧位置处的“ 计算机配置 ”/“ Windows设置 ”/“ 安全设置 ”/“ 本地策略 ”/“ 安全选项 ”组策略分支，并用鼠标双击目标分支下面的“ 网络访问：允许匿名SID/名称转换 ”选项，组策略属性窗口，选中该窗口中的“ 已禁用 ”选项，再单击“ 确定 ”按钮保存好上述设置操作，如此一来任何用户都将不能通过SID标识来远程偷窃本地系统的系统管理员权限账号名称了，那么本地系统的安全性也就得到有效保证了。 编辑推荐： 思科认证更多详细资料 实验:EIGRP浮动汇总路由配置 静态nat与标准acl的混合使用 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