网络信息安全浅析
——Windows XP 系统的安全策略

王 庆，李志蜀
(四川大学 计算机学院，四川 成都 610064)

摘 要：微软公司推出 Windows XP 已有一段时间，显然 Windows XP 在所有关键的性能类别上比起以往其他的 Windows 系统版本都要优越。侧重于分析 Microsoft Windows XP Professional 版本，从其系统本身的特性、服务设置、端口设置及注册表设置等来讲述系统的网络安全策略。

关键词：Windows XP；网络；信息安全；端口；服务
中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1001-3695(2005)02-0014-04

Network Information Security Analysis:
Windows XP System Security Policies

WANG Qing, LI Zhi-shu
(School of Computer Science, Sichuan University, Chengdu Sichuan 610064, China)

Abstract: Microsoft had released Windows XP operating system long before. Windows XP clearly superior to earlier versions of Windows in all key performance categories. This text mainly tells users of Windows XP Professional that how install their operating systemic network secure strategy by modifying systemic services, ports, register-table.
Key words: Windows XP; Network; Information Security; Port; Service

1 概述

Internet 网络的出现标志着人类社会进入了信息化时代。随着计算机、互联网技术的发展，人们的生活已经越来越离不开网络。在 21 世纪的今天，全世界的计算机都可通过 Internet 连到一起，网络安全问题越发显得重要。对于大多数计算机用户，微软公司的 Windows 系列操作系统是首选。Windows XP 自诞生之日起，就以其优秀的人性化界面、众多的功能创新、直观的操作设计、超强的稳定性和可靠的安全性，引起用户的广泛关注。因为 Windows XP Professional 版本适用于大多数用户，在此以 Microsoft Windows XP Professional 版本为例，为企业、家庭及个人用户构建安全的上网方案，提供保护网络信息安全的方法措施。

(1) 使用正版或随机赠送版的操作系统及其他应用软件。盗版的光碟往往带有病毒。有些盗版的操作系统或应用软件一旦安装成功，电脑就感染了某种病毒。最关键的一点，特别对于企业来说，安装大量的盗版软件不仅是违法行为，而且对整个企业内部网络是一种安全隐患。

(2) 及时安装补丁程序。Microsoft 微软公司一旦发现操作系统有漏洞，就会在其官方网站上免费提供相应补丁程序(包)下载。及时安装补丁程序除了增强兼容性外，更重要的是堵上已发现的安全漏洞，消除系统的安全隐患。

(3) 安装正版的杀毒软件。建议选择国产反病毒软件。用户不但可以及时在其网站上升级软件(更新病毒库)，而且可以及时获得许多新病毒或木马的相关信息。当然，选择国际权威反病毒软件也不错，不过它在对付本国土生土长的或新生的病毒方面恐怕不如国产的反病毒软件。另外，安装反病毒软件后必须对其进行必要的设置和时刻开启反病毒实时监控。这样才能有效发挥其最大的威力。

(4) 安装网络防火墙。为了保护计算机系统信息不受外来信息的破坏和威胁，为了防止病毒和黑客的随意入侵，在计算机系统中安装防火墙是很有必要的。Windows XP 系统中新加入了“Internet 连接防火墙”功能，利用该功能，Windows XP 能对出入系统的所有信息进行动态数据包筛选，为内部网络或计算机提供安全保护，一定限度地阻止黑客来访问内部的网络，防止网络上的重要信息被其随意更改、移动甚至删除。不过，其他防火墙与 Windows XP 自带防火墙相比，功能更全面、强大，并且能够定期升级，即及时更新防木马的功能或添加新规则以封堵不必要的和有潜在安全隐患的端口。因此建议关闭 Windows XP 自带的防火墙，而选择安装国产的网络防火墙软件。

(5) 硬盘数据备份。建议用 Ghost 进行备份。Ghost 可以备份整个硬盘，也可以备份某个分区。如果计算机中只安装了一个操作系统，只要将主分区(即 C 盘)备份即可。当计算机的操作系统出现故障而必须重新安装操作系统时，就可以使用 Ghost 的备份文件来恢复硬盘的数据。有条件的用户可以将备份刻录到光盘。另外，还需要制作一张系统启动盘以便必要时使用。需要注意的是 Ghost 备份要求使用 FAT32 的磁盘格式，

收稿日期：2003-12-17；修返日期：2004-09-07

NTFS 就须以其他的办法进行备份。

(6) 屏蔽不必要的服务组件。尽管安装更多的服务组件, 用户就可以享受到更多的服务功能。但是其中有许多是用户根本用不上的, 而那些很少用到的服务不但占用了不少系统资源, 降低了 Windows 系统运行速度, 而且还会为黑客的远程入侵提供了后门, 增加了安全隐患, 为此应该尽量把那些不必要的服务组件屏蔽掉。

(7) 对重要信息进行加密。Windows XP Professional 操作系统中的 NTFS 文件系统有加密文件系统 (EFS) 组件。EFS 是基于公众密钥策略, 对于用户来说, 加密过程是透明, 所以不需要对此有深入的了解就可随时加密文件。在 Windows XP 中可以直接对文件或文件夹进行, 加密时 EFS 自动生成一个加密密钥。不过, 要加密的文件所在的硬盘分区须是 NFTS 格式。Windows XP 中 FAT 32 转换为 NFTS 使用 Convert 命令, 在命令行模式下用 Convert. exe 这个命令随时转换的, 如 Convert c: /fs: ntfs 把 C 盘转换为 NTFS 格式。但此过程不可逆。

满足上述条件, 选中需要加密的文件或文件夹。右击鼠标键, 在随后弹出的快捷菜单中, 选属性选项, 在常规标签中, 点击高级按钮打开高级属性对话框, 选中其中的加密内容以便保护数据选项后, 确定退出即可。

(8) 定期清除 Cookie 缓存、历史记录以及临时文件夹中的内容。上网浏览信息时, 浏览器会把上网过程中所浏览的信息保存在浏览器相关的设置中, 这样下次再访问相同的站点时, 可以提高浏览速度。但是当浏览器的 Cookie 缓存、历史记录以及临时文件夹中的内容保留了用户太多的上网记录时, 这些记录就成了个人信息资料安全的隐患, 所以应该定期清除。

(9) 不随意泄露个人信息。在上网浏览信息时, 经常会遇到需要用户注册个人信息资料的表单。一些站点通过程序设计达到一种用户不填写表单就不能获取所需要信息的目的。在申请 E-mail 邮箱, 使用 OICQ 等一些网络软件及不以游客权限进入 BBS 论坛或聊天室等等的时候, 用户都需要填写一些个人资料。且某些资料被要求必须填写, 无法略过。但对于涉及隐私的资料, 填写要慎重。

(10) 合理设定密码口令。用户在设定密码的时候, 不要直接使用个人和家人的生日, 最好是数字、字母和符号混用, 可以用一些特殊符号, 如@, &, $等, 并且在口令长度允许的范围内, 越长越好。同时用户在不同的地方尽量使用不同的密码, 但务必要把各个对应的密码记下来, 以便查用或更改。

(11) 注意电子邮件的查收。大部分病毒和恶意代码几乎是通过电子邮件传播的。垃圾邮件的增加必然会影响网络安全。特别是对于广告产品的邮件, 用户要小心谨慎, 如果回应这类邮件, 将会导致更多的垃圾邮件。当用户收到一封带有附件的电子邮件, 且附件是扩展名为. EXE 或. ZIP, 切勿轻易执行打开、查看或者保存该附件的命令。

2　Windows XP 系统端口安全设置

Windows 系统提供了很多的服务, 但是用户使用到的毕竟有限。在默认设置条件下, 多种服务会自动启用, 因此无须进行复杂的、特殊的设置就能够使用各种服务, 而有些服务正为居心叵测的人开启了后门。如果任凭某些服务启用, 就很可能成为网络攻击者的攻击对象。安全策略的关键是严格区分必要和不需要的服务, 然后关闭不需要的服务。因为端口往往是绑定着某些服务, 我们可以通过关闭端口来禁用相应的服务。

在默认设置条件下直接运行 Windows 系统, 很多端口就会处于开放状态。一般来说, 端口分为三大类:

(1) 公认端口(Well Known Ports)。从 0 ~1023, 它们紧密地绑定于一些服务。通常这些端口的通信明确对应着某种服务的协议。例如, TCP 端口 21 为 File Transfer Protocol《Control》(FTP 文件传输协议《控制》); UDP 端口 69 为 Trivial File Transfer Protocol(Trivial FTP 小型文件传输协议); TCP 端口 80 为 Hypertext Transfer Protocol(World Wide Web HTTP 全球信息网超文本传输协议) 等等。

(2) 注册端口(Registered Ports)。从 1024 ~49151, 它们松散地绑定于一些服务, 即有许多服务绑定于这些端口。例如, 端口 1024 为 Reserved(保留), 许多服务都可分配到 1024 端口。

(3) 动态或私有端口(Dynamic or Private Ports)。从 49152 ~65535, 理论上, 不为服务分配这些端口。实际上, 2, 3 类端口也可统称为动态端口。这是因为许多系统分配动态端口通常从 1024 左右开始, 即从 1024 端口开始一般不固定分配某种服务, 而是动态分配。动态端口分配是指某个系统进程或应用程序进程根据网络通信的需要, 临时向主机可用的端口号申请一个端口分配给进程使用。当这个进程结束时, 又可以随时释放所占用的端口号。此外, 木马程序多使用这个范围的端口号。如著名的"广外女生"的端口号是 6267, 而"冰河"刚好相反, 端口号是 7626。

因此就必须了解 Windows 系统在默认设置中处于开放状态的具有代表性的端口的作用及其危险性, 并进行适当合理的设置。几乎所有的 Windows 操作系统在默认条件下所开放的端口包括 135, 137, 138 和 139, 而在 Windows XP 专业版中 123, 445, 500, 1900, 5000 端口也是默认开放的。

UDP 端口 123。Network Time Protocol / Simple Network Time Protocol(NTP 网络同步协议)

123 端口用于网络同步, 使网络中的不同的计算机系统实现时间同步服务。此端口对应于服务中的 Windows Time。不需关闭此端口。

端口 135。Remote Procedure Call (RPC 远程过程调用协议) / RPC 终节点映射器

135 端口对应于服务中的 Remote Procedure Call, Event Log 等。135 端口用于启动与远程计算机的远程过程调用(RPC) 连接。RPC 提供了一种进程间的通信机制, 通过这一机制, 允许本地机器上程序进程在远程系统中运行代码。

RPC 在使用 TCP/IP 协议处理信息交换时, 因没有正确地处理畸形的消息而导致存在一个安全漏洞, 即 RPC 接口中远程任意可执行代码漏洞。这是迄今为止 Windows 系统发现的最严重的系统漏洞之一。Windows XP 版本受其影响。

尽管 RPC 终节点映射器侦听 TCP 端口 135, 此缺陷实际上出现在远程过程调用过程中的低级别 DCOM 接口中。RPC 服务在某些情况下无法正确检查消息输入, 导致远程计算机上与 RPC 之间的基础分布式组件对象模型(DCOM) 接口出现问题, 进而使任意代码得以执行。如果向 TCP 端口 135 发送做

了手脚的 RPC 消息,将会因无法正确处理而引发 RPCSS 缓冲区溢出,且允许攻击者执行恶意代码。成功利用此漏洞的攻击者有可能完全获得对远程计算机的控制,即攻击者能够以本地系统权限在系统上执行任意操作指令,如查看文件、更改或删除数据、安装程序、重新格式化硬盘或建立系统管理员权限的新账户等。因为 Windows 各种版本中的 RPC 请求在默认情况下是打开的,这实际上意味着任何能够向受影响的计算机发送 TCP 请求,建立连接的用户都能利用此漏洞。

大名鼎鼎的冲击波(Worm. Blaster) 病毒及其变种就是利用 RPC 漏洞进行传播的。关闭 135 端口,就会将 RCP 服务停止。但是这种绝对的禁止在实际应用中是不可行的,会导致计算机中许多有用的功能不能正常使用,如远程拨号功能等。防范来自 Internet 的远程 RPC 攻击的最佳方法是:将系统打上安全补丁,并在防火墙上设置过滤规则封堵 135 端口。堵住 Windows 系统中的各种技术漏洞,最好的方法就是:进入微软官方网站,下载相应的系统补丁(包) ,及时给系统打上补丁。

UDP 端口 137。NetBIOS Name Resolution(NetBIOS 名称解析)

137 端口对应于服务中的 Computer Browser, Windows Internet Name Service, Server 等。137 端口有管理计算机名的功能。计算机名管理是指 Windows 网络中的电脑通过用于相互识别的名字,即 NetBIOS 名,获取实际的 IP 地址的功能。137 端口会把这种信息包泄漏到网络上。使用 NetBIOS over TCP/IP 时,该端口会自动处于开放状态,由计算机本身向外部散布计算机名称及其用户的详细信息。建议关闭此端口。

UDP 端口 138。NetBIOS Datagram Service(NetBIOS 数据流服务)

138 端口对应于服务中 Computer Browser, Server, Net Logon 等。138 端口和 137 端口一样会向外部发送自己的信息,其特点是会在网络上泄露系统的版本信息。例如,泄漏 Windows 版本是 Windows XP Professional。138 端口还提供 NetBIOS 环境下的计算机名浏览功能,该功能可以让用户在 Browsing List (浏览列表) 里看到连接于网络中所有的计算机。例如,在 Windows XP 中通过网上邻居窗口打开整个网络,将看到一系列的工作组,双击打开某个工作组,就会查看到该工作组里的计算机列表(DoS 方式下可使用命令 net view /domain: workgroupname 查看) 。建议关闭此端口。

TCP 端口 139。NetBIOS Session Service (NetBIOS 会话服务)

139 端口对应于服务中的 Computer Browser, Print Spooler, Server, Net Logon 等。139 端口是基于 SMB 协议(服务器信息块协议) 对外提供共享服务。即通过这个端口进入的连接试图获得 NetBIOS/Server Message Block(服务器信息块) 服务,用于 File and Print Sharing(文件和打印机共享) 和 SAMBA 程序。

TCP 端口 445。Microsoft-DS(透过 IP 的服务器信息块)

445 端口和 139 端口一样都提供局域网中文件和打印机共享服务,不同之处是 445 端口使用 CIFS 协议(通用因特网文件系统协议) 。开放 139 和 445 端口,虽然在网络中有一定的信息安全隐患。但如果用户的计算机需要在内部网络环境中实现文件共享和打印机共享,就不能关闭。反之,则可关闭这两个端口。

关闭 Windows XP 下的 137, 138 和 139 端口。要想停止 NetBIOS 服务,首先由控制面板中选择目前正在使用的网络连接,在属性窗口中查看 Internet 协议(TCP/IP) 的属性。在常规中单击高级按钮,弹出高级 TCP/IP 设置对话框,在 WINS 中选择禁用 TCP/IP 上的 NetBIOS(S) 即可。

对于 139 端口,由于打印机共享服务也是通过它实现,仅停止 NetBIOS over TCP/IP,是不能将其完全关闭的。若将 139 端口彻底关闭,还需要另外的相关设置:打开网上邻居属性框,点击网络任务中的查看网络连接打开网络连接窗口;鼠标右键单击本地连接图标,执行快捷菜单中的属性命令,弹出本地连接属性界面;取消其中 Microsoft 网络的文件和打印机共享选项,再单击确定按钮即可。

而要想关闭 445 端口则必须利用注册表编辑器,在:HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/NetBT/Parameters 中新建名为[SMBDeviceEnabled] 项的 DWORD 值,并将其数值设置为 0,然后退出注册表编辑,重新启动系统。

UDP 端口 500。IPSec ISAKMP(网络安全协议/密钥管理协议)

500 端口提供网络中连接的两台启用了 IPSec (Internet Protocol Security) 的计算机安全关联的建立,指定同一种加密算法和使用同一套通信密钥。Windows XP 系统中 C: /WINDOWS/System32 /lsass. exe 程序使用了此端口,对应于服务中 IPSEC Services。无须关闭此端口。

UDP 端口 1900。SSDP(Simple Service Discovery Protocol 简单服务发现协议)

1900 端口有发现网络服务的功能,可在网络中搜索联机的设备,如网络上的打印机、传真机、扫描器等。由于 SSDP 协议的应用设计上的漏洞,Windows XP 系统会引来 DoS 攻击。此端口与 UPnP(通用即插即用) 服务有关,对应于服务中的 SSDP Discovery Service。建议用防火墙软件屏蔽此端口。

TCP 端口 5000。SSDP Legacy Event Notification (SSDP 继承事件提示)

此动态端口很容易被忽视,但是 Sockets de Troie(国外知名的木马程序) , Bubbel, Back Door Setup 使用了此端口,所以必须注意此端口的开放情况。与其他多数被木马程序侵占的动态端口一样,用户可通过对网络防火墙的规则设置来选择是否屏蔽这些端口,以防止恶意代码的攻击,消除网络中不安全的因素,确保系统的稳定和数据的安全。

3 Windows XP 系统服务安全设置

对于 Windows XP 操作系统,除了直接关闭或开启端口来设置服务外,可以通过服务对话框,进入服务列表,直接对服务进行配置。服务的启动类型分为自动、手动或禁用三种方式。如果服务被配置为自动,则在启动系统时, Windows XP 将自动启动该服务;若被配置为手动,则 Windows XP 无法自动启动该服务,而是在需要该服务时手动启动该服务;若被配置为禁用,则表示不允许启动该服务。在实际配置时,选择手动或者禁用都可以实现关闭该服务的目的。有些服务是 Windows XP 所必需的,不能关闭,否则将会造成系统功能出错,甚至系统崩溃。

而有些服务又是用户用不上的, 可以关闭, 以优化系统设置, 减少入侵后门。了解各项服务的功能, 可以通过双击该服务或将鼠标悬停在该服务名上查看。以下是 Windows XP Professional 版本中一些典型服务的功能与说明:

(1) Alerter(警报器) 。通过服务器发送管理级警报信息到连接在网络中所选定的用户和计算机。

说明: 所用到的端口有 UDP 端口 1900 等。用户是否连接于局域网都不需要计算机系统的管理警报。默认启动类型配置为手动, 可禁用。

(2) Automatic Updates(自动更新) 。实现从 Microsoft 公司官方网站 Windows 更新站点上自动下载 Windows 最新的程序。如果禁用该服务, 用户就不得不在 Windows Update Web 网站查找需要的信息并手动更新。

说明: 为用户下载 Windows 系统的补丁程序、更新驱动程序等提供方便。默认启动类型配置为自动。

(3) Computer Browser(计算机浏览器) 。维护网络上计算机的更新列表, 并将列表提供给计算机指定浏览。

说明: 所用到的端口有 TCP 端口 139、UDP 端口 137 和 138。此服务用于更新或维护计算机网上邻居中整个网络的内容。默认启动类型配置为自动, 但如果用户不想共享自己计算机中的资料, 此服务禁用, 启动类型改为手动。

(4) DHCP Client(DHCP 客户端) 。通过注册和更改 IP 地址以及 DNS 名称来管理网络配置。

说明: DHCP 是动态主机配置协议。用户如果是通过动态分配获取 IP 地址和 DNS 服务器地址的方式连接到网络上, 就不可禁用此功能。否则会导致当计算机登录到网络上时, 只能发送数据包, 而无法接收的情况。默认启动类型配置为自动。

(5) DNS Client (DNS 客户端) 。为计算机解析和缓冲域名系统 (DNS) 名称。如果此服务被停止, 计算机将不能解析 DNS 名称, 也不能定位 Active Directory 域控制器。

说明: 此服务很重要, 不可禁用。默认启动类型配置为自动。

(6) Event Log(错误报告) 。向用户报告来自 Windows 操作系统及程序和组件颁发的事件日志消息, 启用事件查看器查看。

说明: 建议不要终止此系统日志记录服务, 对于快速查找系统问题是很有帮助的。默认启动类型配置为自动。

(7) IPSEC Services(IPSec 服务) 。管理 IP 安全策略以及启动网络密钥交换和 IP 安全驱动程序。

说明: 所用到的端口有 UDP 端口 500 等。IPSec 是网络安全协议, 它能保护网络传输的数据, 保护用户的 TCP/IP 通信免遭窃听和窜改。此服务很有特色, 用户可根据系统自身的安全需要创建和指派 IP 安全策略。默认启动类型配置为自动。

(8) Net Logon(网络登录) 。为网络上授权的用户和服务在本机和域名控制器之间建立安全通路, 并获取登录身份验证和权限。

说明: 所用到的端口有 TCP 端口 139 和 UDP 端口 137, 138 等。默认启动类型配置为自动。如果本机用户不想让局域网上的其他用户登录自己的计算机, 此服务禁用, 启动类型改为手动。

(9) Network Connections(网络连接) 。管理网络连接文件夹中的对象, 在其中可以查看局域网和远程连接的状态。

说明: 此服务禁用, 不会影响用户连接网络, 但网络连接属性将无法正常显示。默认启动类型配置为手动。

(10) Print Spooler(打印后台处理程序) 。管理本机和网络中的打印队列及控制打印任务。

说明: 将文件加载到内存中以便以后打印。默认启动类型配置为自动。要用打印机及传真机的用户不能禁用这项服务。

(11) Remote Procedure Call(远程过程调用 〈RPC〉) 。提供终节点映射程序及为其他基于 RPC 服务提供运行的条件。

说明: 所用到的端口有 135 端口等。RPC 服务很重要, 一般不可禁用。默认启动类型配置为自动。如果一旦将其关闭, 要想恢复此功能, 就必须进入注册表编辑器修改。在 HKEY_LOCAL_MACHINE \System \CurrentControlSet \Services \RPcSs 中的[start] 项的键值已被更改, 只要将其改回 0x00000002(启动类型配置为自动) , 系统重启即可。

(12) Routing and Remote Access(路由和远程访问) 。提供多协议局域网到局域网、局域网到广域网、虚拟专用网(VPN) 及网络地址转换的路由服务。此外, 还提供拨号和 VPN 远程接入服务。

说明: 本机如果不需要作为路由器使用, 此服务禁用。默认启动类型配置为手动。

(13) Server(服务器) 。支持计算机通过网络共享文件、打印和命名管道。

说明: 所用到的端口有 135 端口、445 端口和 UDP 端口 137, 138。如果本机用户不想网络中的其他用户共享自己的资源, 如磁盘、打印机、文件等, 禁用该服务, 断开与远程计算机的所有会话。默认启动类型配置为“自动 ”。

(14) System Restore Service(系统故障恢复服务) 。系统还原是 Windows XP 专业版的一个组件, 执行系统还原功能, 帮助用户恢复丢失的重要文件。

说明: 慎用系统还原功能, 因为消耗了系统大量的资源和内存。要禁用此服务, 从“我的电脑 ”的属性中的系统还原选项卡关闭系统还原。默认启动类型配置为自动。

(15) TCP/IP NetBIOS Helper (TCP/IP NetBIOS 帮助程序) 。为网络计算机用户(客户端) 提供 NetBIOS over TCP/IP 服务以及 NetBIOS 名称解析的支持。

说明: 用户如果不想让别人共享自己的计算机或者不需要 NetBIOS(域名系统) 或 WINS(Windows Internet 名称服务) , 此服务禁用。默认启动类型配置为自动。

(16) Telnet(远程登录) 。允许远程用户登录到计算机系统并运行控制台程序, 支持多种 TCP/IP Telnet 客户, 包括基于 UNIX 和 Windows 的计算机。

说明: Telnet 是进行远程登录的标准协议, 它为用户提供了在本机上完成远程主机工作的能力。不过 Telnet 服务有漏洞, 用户如果不允许远程者登入本机, 也不需要远程控制计算机执行本机控制台命令, 此服务禁用。默认启动类型配置为手动。

(17) Universal Plug and Play Device Host(通用即插即用设备宿主) 。为主机通用即插即用设备提供支持。

说明: 所用到的端口有 TCP 端口 5000 等。早在 2001 年 Microsoft 公司就公布 Windows XP 默认设置下 (下转第 39 页)