Windows 系统安全策略

Windows System Security Policy

朱 敏 （浙江大学网络与信息中心 杭州 310027）

摘要：本文对 Windows 操作系统的安全策略进行了分析，旨在让大家知道在哪些方面执行必要的安全配置，然后根据实际环境再在各个环节分别扩展，最终创建一个安全的 Windows。

关键词：Windows

1 引言

由于 Windows2000 操作系统良好的网络功能，因此有部分网站服务器开始使用 Windows2000 作为主操作系统。但由于该操作系统是一个多用户操作系统，黑客们为了在攻击中隐藏自己，往往会选择 Windows2000 作为首先攻击的对象。

2 如何使系统安全可靠

2.1 禁用 Guest 账号

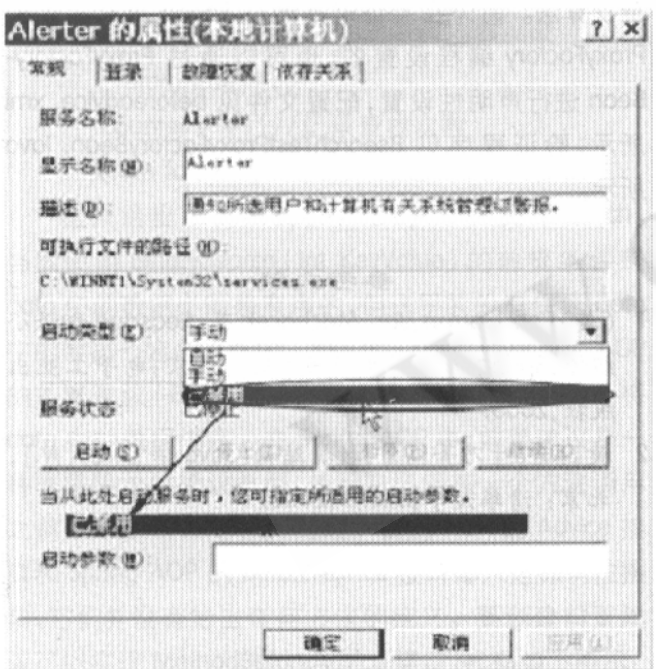

图 1 禁用服务

Guest 账号是一个非常危险的漏洞，因为黑客可以使用这个账号登录你的机器。选择“控制面板”→“管理工具”→“计算机管理”，在计算机管理的“本地用户和组”项，选择“用户”，用鼠标右键单击右侧列表里的“Guest”账号，在右键菜单中选择“属性”或是双击“Guest”账号，属性对话框中，“账户已停用”一项前打勾，这样就无法用 Guest 账号登录系统了。为了保险起见，最好给 Guest 加一个复杂的密码，打开记事本，在里面输入一串包含特殊字符、数字和字母的长字符串，然后把它作为 guest 帐号的密码拷进去。

2.2 限制不必要的用户数量

去掉所有的 duplicate user 帐户、测试用帐户和共享帐号等等。用户组策略设置相应权限，并经常检查系统的帐户，删除已不在使用的帐户。这些帐户很多时候都是黑客入侵系统的突破口，系统的帐户越多，黑客得到合法用户的权限可能性也越大。

2.3 重新配置 Administrator 帐号

Administrator 即超级用户，它的权限至高无上，同时也是被攻击最多的对象。我们要对安装后默认的 Administrator 帐号重新配置，从而达到最大的安全性。建议采取以下措施：

（1）Administrator 重新起名，最好是不起眼的名字。

（2）再创建一个 Administrator 的本地帐号，不分配任何权限，并加上一个超过 10 位的超级复杂密码，以达到诱骗目的。同时经常查看事件日志文件，检查是否有使用这个帐号的企图，从而及早发现攻击隐患。

(3) 使用 passprop 程序为真正的 Administrator 帐号设置帐号锁定策略。

(4) 禁止本地计算机的 Administrator 帐号。

2.4 把共享文件的权限从"EveryOne"组改成"授权用户"

"EveryOne" 在 Windows2000 中意味着任何有权进入你的网络的用户都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成"EveryOne"组。包括打印共享,默认的属性就是"EveryOne"组。

2.5 设置所有磁盘分区的格式都为 NTFS

NTFS 分区磁盘具备高强度的访问控制机制,它能够有效地保护数据不被泄漏与篡改,这是其它格式的分区所不具备的,如 FAT、FAT32 或 FAT32x。因此,要确保服务器上的每个分区都被创建为 NTFS 格式。NTFS 文件系统可以将每个用户允许读写的文件限制在磁盘目录下的任何一个文件夹内,而且 Windows2000 新增的磁盘限额服务还可以控制每个用户允许使用的磁盘空间大小。对已经成为 FAT 格式的分区,可以使用"convert"程序完整地将之转换为 NTFS 格式。但有一点必须提醒,使用"convert"程序时,被转换的磁盘驱动器将被设置为对 Everyone 的 Full 控制权限,这是非常危险的。要解决这个问题,可以使用 Windows NT Server Resource Kit 中提供的"fixacls"软件,它能够帮助我们为驱动器重新配置更为合理的权限。

2.6 禁用不必要的服务

Windows2000 的 Terminal Services(终端服务)、IIS 和 RAS 都可能给系统带来安全漏洞。为了能够在远程方便管理服务器,很多机器的终端服务都是开着的,如果开着的,要确认已正确的配置了终端服务。有些恶意的程序也能以服务方式悄悄的运行。要留意服务器上面开启的所有服务,中期性的检查他们。下面是 C2 级别安装的默认服务:

Computer Browser service TCP/IP NetBIOS Helper
Microsoft DNS server Spooler
NTLM SSP Server
RPC Locator WINS
RPC service Workstation
Netlogon Event log

禁用服务的方法:进入控制面板的"管理工具",运行"服务",进入服务界面,双击屏幕右侧列表中需要禁用的服务,在打开的服务属性的常规标签页"启动类型"一栏,点击小三角形按钮选择"已禁用"如图 1 所示,点击"停止"按钮,最后点击确定即可。禁用服务不但可让系统更加安全,还可让计算机速度运行得更快。

表 1　Windows 2000 禁用服务

服 务	用 途
alerter	通知所选用户和计算机有关系统管理级警报。
clipbook	支持"剪贴簿查看器",以便可从远程剪贴簿查阅剪贴页面。
computer browser	维护网络上计算机的最新列表及提供这个列表给请求的程序。
dhcp client	通过注册和更改 ip 地址以及 dns 名称来管理网络配置。
messenger	发送和接收系统管理员或者"警报器"服务传递的消息。
net logon	支持网络上计算机 pass – through 账户登录身份验证事件。
network dde	提供动态数据交换(dde)的网络传输和安全特性。
network dde dsdm	管理网络 dde 的共享动态数据交换。
runas service	在不同凭据下启用启动过程。
remote registry service	允许远程注册表操作。
server	提供 rpc 支持、文件、打印及命名管道共享。
task scheduler	允许程序在指定时间运行。
tcp/ip netbios helper service	允许对"tcp/ip 上 netbios (netbt)"服务及 netbios 名称解析。
telnet	允许远程用户登录到系统,并使用命令行运行控制台程序。
workstation	提供网络链接和通讯。

2.7 禁用不必要的协议和端口

在配置系统协议时,不需要的协议都可以删除。对于服务器和主机来说,一般只安装 TCP/IP 协议就够了。点击"网络邻居",选择"属性"→"本地连接"→"属性",卸载不必要的协议,如图 2 所示。NETBIOS 是很多安全缺陷的源泉,对于不需要提供文件和打印共享的主机,还可将绑定在 TCP/IP 协议的 NETBIOS 关闭,避免对 NETBIOS 的攻击。选择"TCP/IP 协议"→"属性"→"高级",进入"高级 TCP/IP 设置"对话框,选择"WINS"标签,勾选"禁用 TCP/IP 上的 NETBIOS"一项,如图 3 所示,关闭 NETBIOS。

端口是计算机和外部网络连接的逻辑接口,也是计算机的一道屏障,因此,端口配置正确与否直接影响

表 2　Windows 2003 禁用服务

服 务	用 途
BITS	Background Intelligent Transfer Service
Browser	Computer Browser
Dhcp	DHCP Client
NtLmSsp	NTLM Security Support Provider
NLA	Network Location Awareness
SysmonLog	Performance Logs and Alerts
SrvcSurg	Remote Administration Service
RemoteRegistry	Remote Registry Service
lanmanserver	Server
LmHosts	TCP/IP NetBIOS Helper Service
TermService	Terminal Services
MSIServer	Windows Installer
Wmi	Windows Management Instrumentation Driver Extensions
WMIApSrv	WMI Performance Adapter
ErrRep	Error Reporting

表 3　Windows XP 禁用服务

服 务	用 途
NetMeeting Remote Desktop Sharing	允许授权的用户通过 NetMeeting 在网络上互相访问对方。
Universal Plug and Play Device Host	为通用的即插即用设备提供支持。该项服务存在一个安全漏洞，运行此服务的计算机很容易受到攻击。
Messenger	俗称信使服务，这是一个危险的服务，Messenger 服务基本上是用在企业的网络管理，垃圾邮件和垃圾广告厂商，也经常利用该服务发布弹出式广告。
Terminal Services	允许多位用户连接并控制一台机器。
Remote Registry	使远程用户能修改计算机上的注册表设置。
Fast User Switching Compatibility	在多用户下为需要协助的应用程序提供管理。
Telnet	允许远程用户登录到计算机并运行程序。
Remote Desktop Help Session Manager	如果该服务被终止，远程协助将不能用。
TCP/IP NetBIOS Helper	NetBIOS 在 Win 9X 下经常有人用它来进行攻击，对于不需要文件和打印共享的用户，该项也可禁用。
Error Reporting	服务和应用程序在非标准环境下运行时，允许错误报告。
Print Spooler	将文件加载到内存中以便稍后打印。如果没装打印机，可禁用。

图 2　卸载不必要的协议

到主机的安全。一般仅打开需要使用的端口比较安全。当然，对于文件和打印共享服务的 137、138、139 和 445 端口，还可采用以下的方法来关闭。点击“网络邻居”，选择“属性”，选择“网络和拨号连接”对话框的“高级”菜单，选择“高级设置”命令，进入高级设置对话框，如图 4 所示，在出现的画面中的上部选择所需的连接，下部取消“文件和打印机共享”项（保持空选），即可禁止这几个端口。

另外对于协议和端口的限制，也可采用以下方法：“网上邻居”→“属性”→“本地连接”→“属性”→“Internet 协议（TCP/IP）”→“属性”→“高级”→“选项”→“TCP/IP 筛选”→“属性”，勾选“启用 TCP/IP 筛选”，添加需要的 TCP、UDP 端口和协议即可。由于 Windows 2000 端口过滤有时会阻塞合法的连接，占用的资源多，对主机性能有些影响，所以一般只在网络边界的网关上进行端口过滤，在一般的 Windows 主机上可以不做。

2.8　限制注册表不被匿名访问

默认情况下，注册表可以被远程访问。要限制远程访问，一般只开放 Administrator 的远程访问权限。实现这个目的，需要修改注册表，步骤如下：

(1) 添加下列

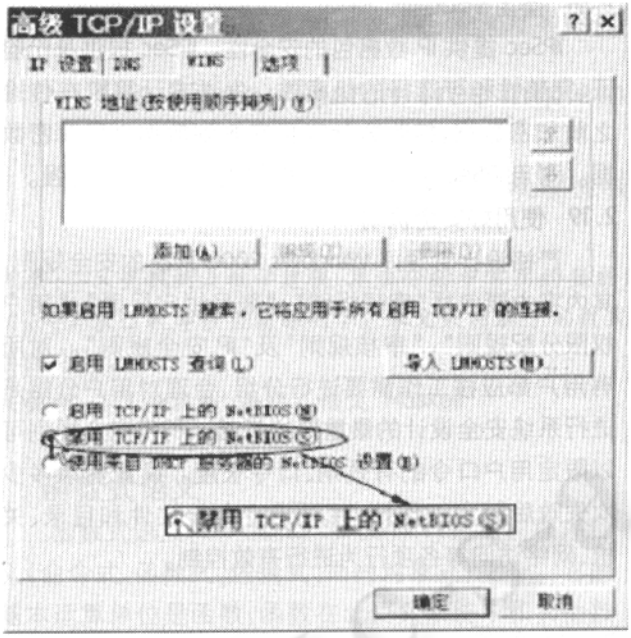

图 3　关闭 NETBIOS

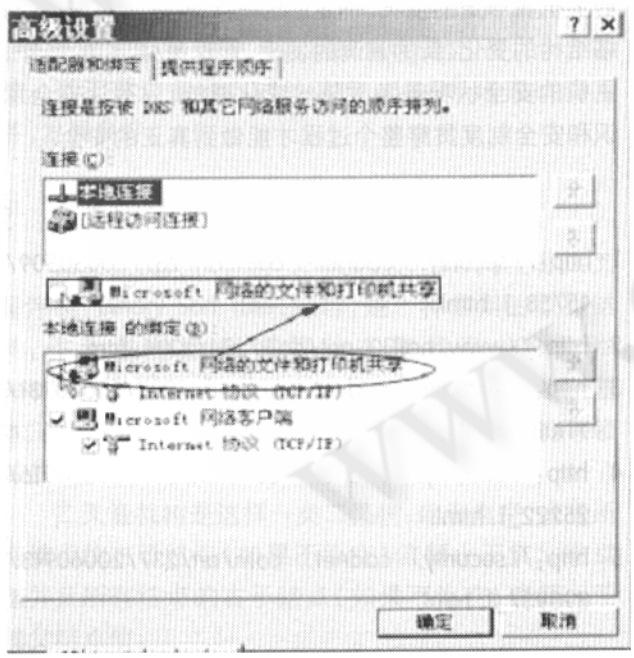

图 4　关闭打印共享端口

key：HKEY_LOCAL_MACHINESYSTEMCurrentControl-SetControlSecurePipeServerswinreg。

(2) 选择 winreg，点击安全(Security)菜单，再点击权限(Permissions)。

(3) 设置 Administrator 的权限为完全控制(Full Control)，并确认列表中没有其他用户或组，点击确定。

通过以上对注册表键值的安全许可设置，就可控制哪些用户或组可以远程访问注册表内容。

2.9 限制 LSA 信息不被匿名访问

LSA 是 Local Security Authority 的缩写，即本地安全颁发机构，它的功能是负责在本地计算机处理用户登录与身份验证。LSA 的信息非常重要，应限制匿名用户对 LSA 的访问。实现这个目的，需要修改注册表，步骤如下：

(1) 创建键值

HKEY _ LOCAL _ MACHINESYSTEMCurrentControl-SetControlLSARestrictAnonymous

(2) 赋值为 1，类型为 REG_DWORD

2.10 预防 DoS

在注册表 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 中更改以下值可以防御一定强度的 DoS 攻击

SynAttackProtect REG_DWORD 2

EnablePMTUDiscovery REG_DWORD 0

NoNameReleaseOnDemand REG_DWORD 1

EnableDeadGWDetect REG_DWORD 0

KeepAliveTime REG_DWORD 300,000

PerformRouterDiscovery REG_DWORD 0

EnableICMPRedirects REG_DWORD 0

2.11 开启审核策略

开启安全审核是 Windows 2000 最基本的入侵检测方法。当系统遭到某些方式(如尝试用户密码、改变帐户策略、未经许可的文件访问等等)入侵的时候，都会被安全审核记录下来。下面这些审核是必须开启的，其他可根据需要增加：

策略 设置

审核系统登陆事件 成功，失败

审核帐户管理 成功，失败

审核登陆事件 成功，失败

审核对象访问 成功

审核策略更改 成功，失败

审核特权使用 成功,失败

审核系统事件 成功,失败

2.12 开启密码策略

策略 设置

密码复杂性要求 启用

密码长度最小值 6 位

强制密码历史 5 次

强制密码历史 42 天

2.13 开启帐户策略

策略 设置

复位帐户锁定计数器 20 分钟

帐户锁定时间 20 分钟

帐户锁定阈值 3 次

2.14 设定安全记录的访问权限

安全记录在默认情况下是没有保护的,把他设置成只有 Administrator 和系统帐户才有权访问。

2.15 不让系统显示上次登陆的用户名

默认情况下,终端服务接入服务器时,登陆对话框中会显示上次登陆的帐户名,本地的登陆对话框也是一样。这使得他人很容易得到系统的一些用户名,进而作密码猜测。修改注册表不让对话框里显示上次登陆的帐户名,步骤如下:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName 把 REG_SZ 的键值改成 1 。

2.16 禁止建立空连接

默认情况下,任何用户通过空连接连上服务器,进而枚举出帐号,猜测密码。可通过修改注册表来禁止建立空连接,步骤如下:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 的 RestrictAnonymous 设置为 1。

2.17 禁止 dump file 的产生

dump 文件在系统崩溃和蓝屏的时候是个很有用的查找问题的资料。然而,它也能给黑客提供一些敏感信息比如一些应用程序的密码等。禁止它,打开"控制面板"→"系统属性"→"高级"→"启动和故障恢复"把写入调试信息改成无。要用的时候,再重新打开。

2.18 使用 IPSec

IPSec 提供 IP 数据包的安全性。IPSec 提供身份验证、完整性和可选择的机密性。发送方计算机在传输之前加密数据,接收方计算机在收到数据之后解密数据。利用 IPSec 可以使得系统的安全性能大大增强。

2.19 使用好安全机制

严格设计管理好 Windows 2000 系统的安全规则,其内容主要包括"密码规则"、"账号锁定规则"、"用户权限分配规则"、"审核规则"及"IP 安全规则"。对所有用户都应按工作需要进行分组,合理对用户分组是进行系统安全设计的最重要的基础。利用安全规则可以限定用户口令的有效期、口令长度。设置登录多少次失败后锁定工作站,并对用户备份文件和目录、关机、网络访问等各项行为进行有效控制。

3 结束语

网络安全是一项系统工程,它不仅有空间的跨度,还有时间的跨度。大多数人认为进行了安全配置的主机就是安全的,其实这其中有个误区。我们只能说一台主机在一定的情况、一定的时间上是安全的,随着网络结构的变化、新的漏洞的发现,管理员/用户的操作,主机的安全状况是随时随地变化着的,只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。

参考文献

1 http://security.ccidnet.com/art/237/20030509/45758_1.html.

2 http://www.net110.net/aqjs/z04/z004.htm.

3 http://security.ccidnet.com/art/237/20060731/711083_1.html.

4 http://security.ccidnet.com/art/237/20020916/25222_1.html.

5 http://security.ccidnet.com/art/237/20060913/898937_1.html.