Windows 2000 信息网络安全与漏洞

刘建炜（长沙中南大学湘雅医学院信息管理系 410078）

摘要 本文主要介绍Windows 2000 信息网络的安全技术和Windows 2000的被黑客利用的一些漏洞及应对策略。

关键词：Windows 2000 信息网络 网络安全

随着信息技术和网络技术的发展，特别是Internet的不断普及，如何防止信息不被非法截获和破坏，即有效维护网络信息的安全性，成为越来越多的人关注的焦点。作为新一代的操作系统的Windows 2000，可通过多种技术和手段来控制用户对资源的访问，提高网络的安全性；对于Windows 2000的强大的功能和全新的构架，可以预见Windows 2000将成为新一代服务器操作系统的主流，同时也成为黑客攻击的对象。但是由于新的Windows 2000的全新构架很大程度都依赖于Active Directory（活动目录），这使得许许多多的管理员在忙于适应新的操作系统和对原来的资料进行系统的迁移，而对Windows 2000的安全性问题还没有引起足够重视，所以黑客常常利用Windows 2000的一些漏洞来攻击Windows 2000系统，本文主要介绍Windows 2000信息网络的安全技术和Windows 2000的被黑客利用的一些漏洞及应对策略。

1 Windows 2000的安全技术

网络和单个系统在Windows 2000下要远比Windows NT 4更加安全。对安全性要求极高的金融机构和其他公司或部门会很满意这个新的操作系统。但是，全面利用Windows 2000的安全性意味着必须使用Active Directory，并且需要相当重视管理并进行重要的培训。

Windows 2000的安全技术包括与活动目录（Active Directory）服务的集成，支持认证Windows 2000用户的Kerberos v5认证协议，提供了公钥基础设施PKI支持，用公钥证书对外部用户进行认证，使用加密文件系统EFS（Encrypting File System）保护本地数据以及使用Internet协议安全（IPSec）来保证通过公有网络的通信的安全性，以及基于Windows 2000的安全应用开发的可扩展性等。

在Windows 2000安全结构和框架中，除了能够保护网络资源和硬盘资源的合法使用以外，还应该提供多种技术来保证网络传输数据的安全性。为满足这种需求，Windows 2000中集成了对IPSec的支持。

IPSec是一组Internet标准协议，可以在非安全网络之间建立安全通道，对传输的信息进行安全处理。IPSec的加密技术应用于网络的IP层，所以，对于大部分使用特定网络通信协议的上层应用来说都是透明的。IPSec提供了端到端的安全性，也就是说由发送端计算机加密的IP包只能被接收端计算机解密，中间截获的数据都是不可读的。

IPSec提供了如下安全功能：

(1) 在Kerberos认证、数字证书或共享密钥的基础上认证IP数据包的发送者。

(2) 保证IP数据包在网络传输过程中的完整性。

(3) 对通过网络传输的所有信息进行加密，以保证数据的机密性。

(4) 在数据传输过程中，可以隐藏数据的原始IP地址。

所以，Windows 2000使用IPSec，可以充分保障网络数据传输的机密性、认证性、完整性和不可否认性。

另外，Windows 2000中还提供了其他的网络和信息安全技术支持，如虚拟专用网VPN支持和Internet验证服务等。所以，通过对Windows 2000的合理化管理和配置，可以在现有投资的情况下有效保证网络信息的安全性。

2 Windows 2000的漏洞

2.1 登陆输入法漏洞

首先介绍一个登录错误，也就是常说的输入法漏洞。当我们启动Windows 2000进行到登录验证的提示界面时，任何用户都可以打开各种输入法的帮助栏，并且可以利用其中具有的一些功能访问文件系统，这也就是说我们可以绕过了Windows 2000的用户登录验证机制，并且能以最高管理员权限访问整个系统。所以说这个漏洞的危害性是很大的，而且当我们进入系统后，还可以利用Terminal Server远程通信这个漏洞对系统进行攻击。默认的Windows 2000系统自带的输入法中有这个漏洞的是：智能ABC，微软拼音，内码，全拼，双拼，郑码。所以就我感觉而言这个漏洞是首要修补的漏洞。

(1) 把不需要的输入法删除掉，例如郑码等。

(2) 但毕竟我们不能把所有的自带输入法都删除，若我们要使用有漏洞的输入法可以把那个输入法的帮助文件删除掉，这些帮助文件通常在win2000的安装目录下的help目录下。

(3) 微软公司对于此问题发布了MS00-069安全公告，并在互联网上给出了简体中文Windows 2000和英文版Windows 2000的补丁。所以应尽快打上补丁。

2.2 NetBIOS的信息泄漏

NetBIOS的共享入侵这个问题从NT刚发行到现在就从来没有解决。而且它一直都是NT系统构架最常见的入侵手段。特别值得一提的是那个IPC$Null session（空会话）在NT系统里都是已知的安全隐患，虽然打了SP3后可以通过修改注册表来对其进行限制，但不知道为什么Windows 2000还是原封不动地保留着这个空对话。那么就让我们

来看看空会话能给入侵者带来什么样的信息：

net use \\server\IPC$ "" /user:"" //此命令用来建立一个空会话

net view \\server //此命令用来查看远程服务器的共享资源

服务器名称 注释

\\pc1

\\pc2

命令成功完成。

net time \\server //此命令用来得到一个远程服务器的当前时间。

nbtstat -A server //此命令用来得到远程服务器的NetBIOS用户名字表

NetBIOS Remote Machine Name Table

Name	Type	Status
NULL	<00> UNIQUE	Registered
NULL	<20> UNIQUE	Registered
INTERNET	<00> GROUP	Registered
XIXI	<03> UNIQUE	Registered
INet~Services	<1C> GROUP	Registered
IS~NULL.....	<00> UNIQUE	Registered
INTERNET	<1E> GROUP	Registered
ADMINISTATOR	<03> UNIQUE	Registered
INTERNET	<1D> UNIQUE	Registered
.._MSBROWSE_.	<01> GROUP	Registered

MAC Address = 00-54-4F-34-D8-80

看看，只不过用了几个系统自带的命令就得到了如此多的信息，那么我们有什么办法可以不让别人轻易得到这么多信息呢？

仅靠单纯的修改注册表是一劳永逸的。

HKEY-LOCAL_MACHINE\SYSTEM\CurrentControSet\Control\LSA

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Value: 1

但如果一些服务你并不需要开放共享的话，那么就禁止共享。在Windows 2000里的方法和NT4的略有不同。它没有限制TCP/IP绑定在NetBISO上，但是我们可以在Internet协议(TCP/IP)属性的设置面板里选取高级(V)选项，然后选择TCP/IP筛选，接着点选启用TCP/IP筛选，最后在TCP端口点选只允许，然后就可以添加你所想开放的服务的端口了。

2.3 奇怪的系统崩溃特性

Windows 2000有一个比较奇怪的特性，使用系统的终端用户可以通过按住右Ctrl，同时按两次Scroll Lock按键，就轻易可以让整个Windows2000系统完全的崩溃。但同时又在C:\WinNT\下dump完整的当前系统内存记录，内存记录文件名是memory.dmp。当然，这个奇怪的特性默认状态下是关闭的，这个特性在WindowsNT4中也存在，不知道是不是微软程序员作测试的一个小功能。不过要是有黑客或者病毒利用它，也是很危险的。

2.4 Telnet的拒绝服务攻击

Windows中的Telnet一直以来都是网络管理员们最喜爱的网络实用工具之一，但是一个新的漏洞表明，在Windows 2000中Telnet在守护其进程时，在已经被初始化的会话还未被复位的情况下很容易受到一种拒绝服务的攻击。

Telnet连接后，在初始化的对话还未被复位的情况下，在一定的时间间隔之后，此时如果连接用户还没有提供登录的用户名及密码，Telnet的对话将会超时，直到用户输入一个字符之后连接才会被复位。如果恶意用户连接到Windows 2000的Telnet守护进程中，并且对该连接不进行复位的话，他就可以有效地拒绝其他的任何用户连接该Telnet服务器，主要是因为此时Telnet的客户连接数的最大值是1。在此期间任何其他试图连接该Telnet服务器的用户都将会收到如下错误信息：

Microsoft Windows Workstation allows only 1 Telnet Client LicenseServer has closed connection

察看"列出当前用户"选项时并不会显示超时的会话，因为该会话还没有成功地通过认证。

2.5 IIS服务泄漏文件内容

这是一个Nsfocus安全小组发现的漏洞。当微软IIS 4.0/5.0(远东地区版本)在处理包含有不完整的双字节编码字符的http命令请求时，会导致Web目录下的文件内容被泄漏给远程攻击者。

Microsoft IIS远东地区版本包括中文(简体/繁体)，日文，韩文版，由于特定的文字格式使它们都是使用的双字节编码格式。而当IIS接收到用户提交的一个http请求时，如果文件名中包含非ASCII字符，IIS会检查这个字符是否为双字节编码中的前导字符(例如，日文的前导字符包含两段字符：0x81-0x9F，0xE0-0xFC)。如果是前导字符，它会继续检查下一个字符是否为结尾字符。如果没有下一个字符，IIS会简单地丢弃这个前导字符，因为它并没有构成一个完整的双字节编码。然而，这种处理将导致IIS打开不同的文件而不是用户在请求中指定的文件。

黑客是利用Unicode(统一的字符编码标准，为双字节编码)漏洞配合IIS的漏洞进行入侵的。

黑客其实只要用下面两句很简单的指令绕过IIS的审计就能够对网站的页面进行改写，所谓的黑了一个网站就是这么的简单。

http://server/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+d:\inetpub\scripts\123.exe

http://server/scripts/123.exe?/c+echo+黑掉啦?+>+c:\inetpub\wwwroot\default.asp

这个问题已经在IIS 4.0 + SP6中得到解决，然而微软却让它在IIS 5.0中再度出现，但该漏洞不会影响包括英语版在内的其他西文版本的IIS 4.0/5.0。

2.6 MS SQL Server的SA空密码攻击

在Windows 2000中，企业级的用户一般都会用到数据库管理软件MS SQL Server，但是在与MS SQL Server配合使用中，我们发现了很多的问题。最后我们就简单讲一下安装了MS SQL Server的Windows 2000的网络操作系统普遍面临的安全问题。

在安装MS SQL Server后，MS SQL Server会将产生一个默认的SA用户，而且初始密码在管理员没有设置的情况下为空。但是SA是SQL Server中非常重要的安全模块成员，这样一来黑客们就可以通过SQL Server的客户端进行数据库远程连接，然后再通过SQL的远程数据库管理命令xp_cmdshell stored procedure(扩展存储过程)来进行命令操作：

xp_cmdshell "net user id password /add"

Xp_cmdshell "net localgroup Administrators

id /add"

就以上两条简单的命令入侵者就能在MS SQL Server的服务器上马上新建一个管理员级别的Administrators组的用户，所以我们这里提醒各位网管，在安装好SQL Server您需要做的第一件事就是把SA的空密码立即进行修改。

2.7 Windows媒体播放器漏洞

微软的Windows媒体播放器的"skins"中有重大安全漏洞。"skins"是用来设定台式机应用软件的用户画面的。攻击者可利用它的安全弱点，阅读本机文件、浏览目录、甚至可随意终止用户使用和程序。这样攻击者可完全控制用户的机器，并可随心所欲地使用用户的机器。下载一个Java applets的程序到微软的媒体播放器的目录里，就会出现这个漏洞。因为微软的媒体播放器及IE都不拒绝应用软件。

这个漏洞用户自己可以进行安全保护。在IE中的"互联网"选项中，用户可以禁止任何Java的内容。这样用户就可免受攻击。

以上讲述了几个近期来最为流行的漏洞和攻击方法，他们实现入侵是如此的方便，但只要我们常留意微软的补丁包文件，并注意及时的把系统和软件更新到最新的补丁；正确给系统加设密码，系统的安全率就可达85%左右。

3 Windows 2000的安全设置

从前面的分析可知，Windows 2000的安全设置的重要性。以下简单谈谈自安装开始系统的安全设置问题。

3.1 系统的安装

在系统安装过程中主要要注意以下几点：

(1) 硬盘的分区。至少建立两个逻辑分区，一个用作系统分区，另一个用作应用程序分区，现在的硬盘是越来越大，一般最好分三至四个分区，这样就可以把自己的文件单独放在一个分区中。文件分区最好采用NTFS格式，因为这种文件格式的分区在安全性方面更加有保障，至少是系统分区中应是如此。

(2) 系统版本的选择。Windows系统的内核语言是英语，这样相对来说它的内核版本比其他语言的编译版本中的BUG少，所以如果是在单位网络中用Windows 2000，最好选用原英文版，这样选择的好处还在于将来升级、加补丁也远比其他语言版本快。

(3) 正确的网络接入时间。我们都有这样一个坏习惯，那就是在安装系统之前我们会把一切硬件都连接好，这主要是方便系统的安装，但在安装Windows 2000时要注意，最好在系统未全部安装完全之前不要连入网络，特别是Internet。因为Windows 2000在安装时有一个漏洞，就是在输入用户管理员账号"Administrator"的密码后，系统会建立"$ADMIN"的共享账号码，但是并没有用刚输入的密码来保护它，这种情况一直会持续到计算机再次启动。在此期间，任何人都可以通过"$ADMIN"进入系统；同时，只要安装一完成，各种服务就会自动运行，而这时的服务器还到处是漏洞，非常容易从外部侵入。因此，在完全安装并配置好Win2000 Server之前，一定不要把主机接入网络。

3.2 系统及应用软件安全设置

(1) 用户账号的安全设置。在一个局域网中，正确有效地设置各不同组用户账号的权限，是确保网络安全的首要因素。Windows 2000的默认安装允许所有用户通过空用户名和空密码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，同时任何一个远程用户也可以通过同样的方法得到你的用户列表，并可能破解用户密码给整个网络带来破坏，这是整个网络中的最大不安全因素之一。

(2) 文件和文件夹权限的设置。我们知道NT系统的安全性在本地网络中最主要还是可以自由设置各用户、文件和文件夹的访问权限来保证的。为了控制好服务器上用户的权限，同时也为了预防以后可能的入侵和溢出，必须安全有效地设置文件夹和文件的访问权限。NT的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。在默认的情况下，大多数的文件夹和文件对所有用户是完全控制的，这根本不能满足不同网络的权限设置需求，所以你还需要根据应用的需要进行重新设置。

要正确有效地设置好系统文件或文件夹的访问权限，必需注意NTFS文件夹和文件权限具有继承性、累加性、优先性等属性。

3.3 设置好IIS

IIS是微软的组件中问题最多的一个，要注意很多软件的默认安装是黑客攻击的源头，是引起不安全因素的根源，微软的IIS也不例外，同时它又是一个网络应用软件，直接与千变万化的互联网相联系，所以IIS是我们安全配置的重点。

首先，为了系统的安全起见我们一般要删除系统盘下的Inetpub目录，在另一分区中新建一个Inetpub，并使IIS管理器中将主目录指向它，这样即使IIS安全出了问题，也不会直接影响到整个系统。

其次，我们要记住一个原则，那就是：最小的权限+最少的服务=最大的安全。所以必需把IIS安装时默认的scripts等虚拟目录也一概删除，如果你需要什么权限的目录可以以后再建。

然后是应用程序的配置。在IIS管理器中把无用映射都统统删除(当然必须保留如ASP、ASA等)，在IIS管理器中"主机→属性→WWW服务编辑→主目录配置→应用程序映射"，然后开始一个个删掉。接着再在应用程序调试书签内，将"脚本错误消息"改为"发送文本"，点击"确定"退出时别忘了让虚拟站点继承刚才设定好的属性。

最后，为了保险起见，可以使用IIS的备份功能，将刚刚的设定全部备份下来，这样就可以随时恢复IIS的安全配置。

还要强调的是：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。很多朋友认为进行了安全配置的主机就是安全的，其实这是个误区，我们只能说一台主机在一定的情况下一定的时间内是安全的，随着网络结构的变化、新的漏洞的发现、管理员和用户的操作，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 健莲工作室，Windows 2000中文版网络与通信专辑，人民邮电出版社，2000年。

2 中华技术网，http://www.asfocus.com。