操作系统安全简论——Windows NT操作系统安全（五）

卿斯汉 （中科院信息安全技术工程研究中心 100080）

漏洞37：当Windows NT系统管理员远程向域内增加帐号的时候，管理员所在主机名以明文方式跟随在被增加帐号密文口令之后，远程增加帐号时的缺省口令是管理员所在主机名本身。利用这个信息，可以获取管理员目前使用的用户会话密钥，该密钥被管理员用于加密到PDC的数据传输，包括更改的口令信息。对于LanManager Version 1，这个用户会话密钥是Windows NT口令的单向Hash函数，因此，除非系统管理员更改自己的口令，该会话密钥始终有效。对于LanManager Version 2，这个用户会话密钥是基于随机数据的，并且每次连接都会重新创建，因此仅仅在当前会话中有效。

对策：NTLM（所有版本）：所有帐号更改操作都在PDC上完成，或者经由安全信道远程更新。如果上述要求无法满足，应该在每次远程更新帐号前后强制产生新的用户会话密钥。NTLM v1：在PDC上更改administrator口令，NTLM v2：按如下步骤切断后重新连接远程主机：终止一切存在到PDC连接的应用程序、服务等等，输入"net use"观察当前连接。如果存在一个到"\\PDC\ipc$"的连接，用"net use \\mypdc\ipc$ /del"切断它。

漏洞38：WinNT/2000中的SNMP协议允许管理员从远程管理网络设备。这是通过创建注册表设置（HKEY-LOCAL-MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters）并指定授权的管理员的IP地址或机器名实现的。这些SNMP权限设置都保存在网络设备本地。所有的网络设备按照community进行分组。通常，具有管理权限的用户修改注册表键的设置。但是，由于SNMP注册表键的权限的默认配置存在错误，任何可登录机器的用户都可以修改这些设置，成功地利用这个漏洞将允许用户完全控制网络设备。

对策：微软已经发布如下补丁修正该漏洞：

Microsoft Windows NT 4.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24501

Microsoft Windows 2000：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24500

漏洞39：如果用户本地登录到一台Windows 2000机器，在某些特定条件下，可以获得对其他用户的widnows stations进程的访问权限，这将允许一个低级别的用户的进程看到同一个session中另外一个桌面的输入或输出数据，可能包含口令等敏感信息。

对策：微软已经发布了一个相应的补丁程序，可以在下列地址下载：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20836

漏洞40：在主域控制器和备份域控制器（PDC/BDC）进行同步的时候，SAM数据库被加密后传送。每次同步之时，都会产生一个唯一的RC4加密字串。LM和NT的Hash值与帐号的RID有关，并且LM和NT的Hash使用同一个RC4加密字串进行异或操作，在某些特定条件下，例如主机重设了一个可信帐号的口令，则NT Hash值会被正常传输，而LM Hash值则被设置为16个零字节，因此这16个字节与RC4加密字串异或以后得到的仍然是相应的原值（16字节），如果攻击者能够监听到这个数据，就知道主域控制器和备份域控制器进行同步时用的RC4加密字串，就有可能利用它解出SAM数据库中的所有帐号的LM Hash值，再用其他的解密软件解出LM口令。

对策：升级到Service Pack 4或者更高版本。

漏洞41：在远程主机对注册表的访问请求被处理前，需要先经由远程注册表server进行认证，如果提交一个错误格式的请求，将使远程注册表server发生错误，不能正常工作。在Windows NT 4.0中，由于注册表server包含在winlogon.exe系统进程中，这个进程出错将导致整个系统不可用。注意，只有一个已经通过认证的用户才能发起这样的请求，匿名（空会话）连接不能导致这种拒绝服务攻击，受到攻击的系统必须重新启动才能正常工作。

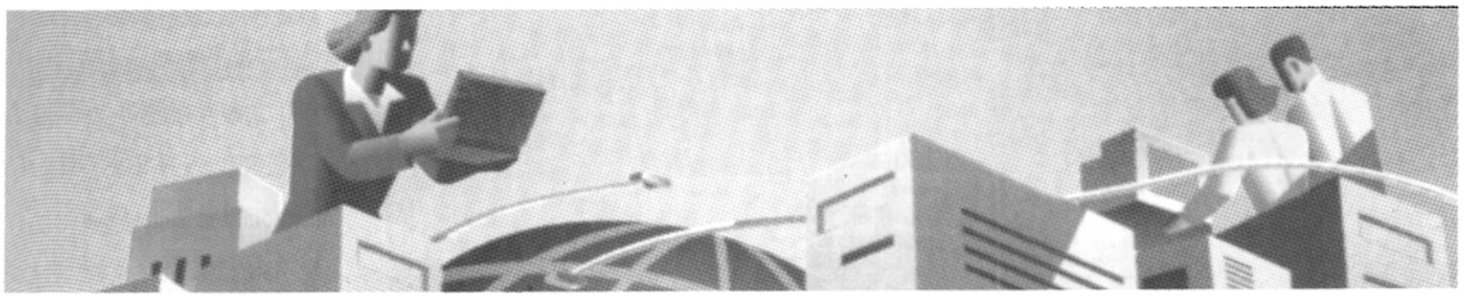
对策：微软已经提供了针对Microsoft Windows NT 4.0 Workstation、Server和Server Enterprise Edition的补丁，可以在下列地址下载：http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21772

漏洞42：Microsoft Windows NT 4.0中计算机的浏览协议，没有对加入主浏览器浏览列表中的主机数量进行限制，恶意用户可以向主浏览器发送大量伪造的主机宣称数据帧（HostAnnouncement frames），形成对主浏览器的flood攻击，同时造成对进行网络浏览的客户端的拒绝服务攻击，这些包也会占用大量的网络带宽，降低网络性能。

对策：微软已经提供了补丁，可以在下列地址下载：

Windows NT 4.0 Workstation, Server, and Server, Enterprise Edition：

http://www.microsoft.com/Downloads/Release.



asp?ReleaseID=21397

Windows 2000：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21298

漏洞43：微软Windows 2000中的RPC服务存在一个内在的缺陷，因此可能使Windows 2000 server的RPC服务崩溃，从而使后来的任何RPC请求都遭到拒绝。通过135～139或445端口给Windows 2000 server发送一个特殊构造的RPC包将会使RPC服务完全停止，恢复正常功能必须重启机器。

对策：微软已经发布如下补丁消除本漏洞：

http://www.microsoft.com/technet/security/bulletin/fq00-066.asp

漏洞44：微软Windows 2000中，一个Active X控件存在一个未经检查的缓冲区，根据激活该Active X控件时输入的数据的不同，恶意用户可对远程系统发起拒绝服务攻击或者在远程系统上执行任意代码。这个漏洞可通过两种方法加以利用，即通过web或兼容HTML的邮件。漏洞代码将以远程系统中当前用户的特权等级运行。

对策：微软已经提供补丁消除该漏洞：

Microsoft Windows NT 2000：

Microsoft patch Q278511-W2K-SP2-x86-en (http://download.microsoft.com / download-/ win2000platform/ Patch/ Q278511/NT5/EN-US/ Q278511-W2K-SP2-x86-en.EXE)

漏洞45：在特定情况下，有可能在本地机器上绕过域帐号锁定策略，使这种保护手段对于穷举式密码攻击尝试不再有效。域帐号锁定策略的目的是，在一定次数的不成功登录尝试之后禁止该帐号。如果没有实现这种策略，则可以对域帐号的密码进行无穷多次猜测。在一个使用NTLM认证的非2000域中，Windows 2000主机无法识别针对那些凭证缓存，本地用户制订的域帐号锁定策略。缓存的凭证包括用户名和以散列值形式存放的密码。在域控制器无法实施认证的情况下，缓存的凭证将被使用。不使用NTLM进行认证的Windows 2000系统不受本漏洞的影响，因此作为Windows 2000域成员的客户端不存在本漏洞(它们实现的是Kerberos认证)。

对策：微软已经发布如下补丁消除本漏洞：

Microsoft Windows NT 2000：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25606

5.2 Windows NT常用软件的安全漏洞及对策

漏洞1：通过Internet Explorer 5.X访问FTP站点，密码和用户名都是以文本方式的形式存储在历史记录中的：

英文版：

\Winnt\Profiles\[Username]\History\History.IE5\index.dat and

\Winnt\Profiles\[Username]\History\History.IE5\MSHist<date>..\index.dat。

中文版：

\Winnt\Profiles\[Username]\Cookies\index.dat。

默认的情况下，\Winnt\Profiles\[Username]\History目录，只有管理员组和目录所属用户有完全管理的权限。然而，index.bat可以被任何人访问，因为"Bypass Traverse Checking"的权限默认是赋给每一个组的。因此，任何一个用户都可以访问主机，并读取另外一个用户的index.dat文件。

对策：

(1) 除了管理员外，其他人都将"Bypass Traverse Checking"去掉。

(2) 对每个用户的配置中的目录和文件设置访问控制，只允许所有者(或管理员)访问。

(3) 如果历史记录中包含密码等敏感信息，将其删掉。

(4) 直接用FTP客户端完成FTP功能，而不用IE。

漏洞2：Internet Explore在某些情况下，随意向Internet上发送用户的名字和口令，这种对身份验证的自动反映和发送对用户来说，是完全透明的。

当访问一个兼容的WWW服务器(比如Microsoft的IIS服务器)时，Windows NT平台上的Internet Explore将会对SMB协议自动反应，发送用户的名字和加密的口令，用户根本不知道什么事情发生。

对策：安装Microsoft的最新补包，据说已经解决了这个问题。

漏洞3：Windows NT和Windows 95机器上的所有浏览器，都有一个相似的弱点，对于一个HTML页上的超级链接，浏览器都首先假设该链接是指向本机器上的一个文件。如果这台机器是一个SMB服务器，它将随意发送用户的名字和口令，这种对身份验证的自动反应和发送对用户来说，是完全透明的。

如果一个HTML页有这样一个链接，如file://IP-address/path-and-filename嵌入在HTML代码之中，浏览器将假设该链接是指向本机器上的一个文件，然后自动地试图接上该链接。如果这台

机器是一个 SMB 服务器，本地机器将试图进行身份验证，它将随意发送用户的名字和口令。这种对身份验证的自动反应和发送对用户来说，是完全透明的。用户根本不知道什么事情发生。

对策：由于这种反应只发生在 TCP 和 UDP 端口 135 至 142 上，建议在防火墙上，截断所有这些端口。另外，在内部路由器上，设置 ACL，在各个独立子网之间，截断从端口 135 至 142 的连接。这是一种辅助措施。

漏洞 4：ASP 数据流的弱点，它主要影响如下系统：Microsoft Internet Information Server version 1.0，2.0, 3.0, 4.0；Microsoft Peer WWW Server version 2.0, 3.0; Microsoft Personal WWW Server version 4.0 on Windows NT 4.0 Workstation。

问题是在微软的 IIS 中发现的，WWW 客户可以读出 IIS 目录中任何一个 NTFS 文件的内容，这些文件通常被赋予 "读访问" 的权限，其中包括 ASP 程序。主数据流具有一个属性叫做 $DATA。从浏览器访问 IIS 上的这个 NTFS 流，可以显示出一个文件的内容，这种方式通常被应用程序映像 (Application Mapping) 所利用。这可使一般用户下载.ASP 文件，从而得到源程序代码。然而，它并不允许用户在服务器端修改 .ASP 文件，从而得到源程序代码。很容易验证 IIS 的这个弱点，选择一个带有 .ASP 扩展名的 URL，然后附加上字符串 "::$DATA"。例如：

http://www.domain.com/scripts/test.asp::$DATA

你将看见的不是 test.asp 执行后的输出，而是 test.asp 的源程序代码，或者弹出一对话框，让你保存。

对策：微软已于 1998 年 7 月 3 日在其安全站点上，发布了关于 IIS3.0 和 IIS4.0 的补丁包。另外，也介绍了关于 $DATA 问题工作情况的进展。IIS 早期版本的用户应该考虑升级到 IIS 的近期版本 (3.0 或 4.0)。如果用户自己无法应用以上补丁包，可以把所有 .ASP 文件对非管理员用户的 "读" 权限先行去除，只保留其 "执行" 权限。如果把整个站点的 "读" 权限去掉，所有的文件 (包括 .htm, .gif, .asp, .jpg 等) 将不可读，用户将无法访问你的站点。事实上，ASP 文件只需要 "执行" 权限，而对于非执行文件，它们通常有 "读" 权限就可以满足显示的需要了。另外，还要修改相应的应用程序映像 (Application Mapping)，使其包含 "::$DATA"。

漏洞 5：IE 读出本地文件，它主要影响如下系统：

Microsoft Internet Explore 4.0，4.01 SPI for Windows NT 4.0,Windows 95

Microsoft Windows 98, with Internet Explore 4.01 SPI

Microsoft Internet Explore 4.0，4.01 for Windows 3.1, Windows NT 3.51,Macintosh

Microsoft Internet Explore 3.x

在 Internet Explore 3, 4.0, 4.01 中存在一个 Bug，允许特别设计的 WWW 网页读出计算机上的文本文件或者 HTML 文件，并且把这些文件发送到指定主机甚至可以穿越用户端的防火墙。这个 Bug 使用 JavaScript 进行编程，并且事先知道文件名和存储位置。另外，这个 Bug 还允许把特别设计的消息发送给某个 Outlook Express 或 IE4 用户。

根据微软的安全公告板，这个漏洞允许一名恶意的黑客绕过 IE 的安全机制，使恶意的 WWW 站点操作员能够读出用户电脑上的文件内容。微软称这个 Bug 为交叉帧导航问题(Cross Frame Navigate Vulnerability)。NTSecurity.net 也详细报告了这个问题，并且给出了检查 mshtm.dll 文件是否被感染的详细操作步骤。

对策：微软于 1998 年 9 月 4 日发布了补丁包解决这个问题。这些补丁包可以从微软的站点下载。微软强烈建议受影响的用户 (列在受影响的版本中)，应该尽早下载并且安装这些补丁包。对于 IE4.x，这些用户应该从下述安全站点上下载补丁包：

http://WWW.microsofu.com/ie/security/xframe.htm

Windows 98 的用户可以通过使用 Windows Update 的功能来获得补丁包。对于 IE3 的用户，首先应该升级到 IE 的最近的版本，然后再安装 IE4 的补丁包。升级信息详见于 IE 的下载站点：http://WWW.microsofu.com/ie/download

漏洞 6：IIS 的 FTP 拒绝服务，它主要影响如下系统

Internet Information Server 2.0, 3.0, 4.0

IIS 的 FTP 服务采用被动模式 (PASV)，可能导致性能的下降，甚至导致遭受 FTP 和 WWW 的拒绝服务攻击。当有问题发生时，系统审计文件会显示这样一条出错信息：

FTP Server could not create a client worker thread for user at host. The connection to this user is terminated. The data is the error.

客户端的系统也会看到出错信息，如：

Connection closed by remote host. 或者 The FTP session was terminated.

另外，还有一个 FTP 的 DoS 问题是由 Marcos Guillen 报告的。如果一个 IIS4.0 服务器上的 FTP 服务设立了超过 100 个不同的 FTP 虚拟目录或者虚拟站点，很容易遭受 DoS 的攻击，这类攻击往往同时发送 10 个以上的 PUT 或者 DELETE 命令给某个 FTP 公共目录。这时，FTP 服务器会显示一条出错信息："426 Connection closed: transfer aborted"，这条信息会发送给所有在这台机器上 FTP 的公共或者私有的虚拟目录、虚拟站点，终止对任何一名用户的服务，包括系统管理员。这时，只有重新启动 IIS 的服务，才能解决这个问题。

对策：下载并安装微软的补丁包。在下载时，请注意 IIS 的版本。补丁包的路径是：

ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes

上述漏洞并没有列出 Windows NT 的全部漏洞，一些新的漏洞将会随时被发现。作为 Windows NT 的使用者，应密切注视微软公司的安全公告牌及其他安全公告，随时对漏洞进行修补。同时，合理地设置本系统的安全配置，也可以防止黑客对某些漏洞的攻击。