

谈网络环境下图书馆工作用机常见的安全问题和防护措施

王纪英 王艳翠

山东聊城大学图书馆

【摘要】 详细阐述了网络环境下图书馆工作用机的系统漏洞及流行病毒的危害和相应的防护措施,为图书馆网络的安全维护提供一个必要的参考。

【关键词】 资源共享 系统漏洞 网络病毒 安全维护 用户教育

随着图书馆网络的普及和飞速发展,对网络环境下工作用机的安全防护已成为一个非常重要的课题。为此,作者对 Windows 操作系统存在的常见漏洞和目前网络流行病毒的传播途径、发作状况和安全防护措施进行了详细的报道,为网络环境下图书馆工作用机的安全维护提供一个必要的参考。

1 常见 Windows 系统漏洞及其防护措施

1.1 资源共享漏洞 通过资源共享可以轻松地实现对远程计算机的访问,但其中存在着不少漏洞。只要将其“访问类型”设置为“完全”方式,用户就可以任意上传、下载,甚至是删除远程计算机共享文件夹的文件。如果再上传并激活一个设置好的木马程序,则可以得到远程电脑的控制权。

将“访问类型”设置为“根据密码访问”,可以有效地避开这一漏洞。然而,在 Windows98 下用户可以利用系统的另一漏洞绕过密码而登录(该漏洞在 Windows2000 已得到解决)。另外,有些用户

设置“共享名(N)”时常使用“\$共享名”技巧,即在共享名后面加 \$ 符号,如“CS\$”、“DS\$”等。这样共享信息是不会有在电脑中显示出来的,必须正确地键入共享名才能正常浏览,如“\ \ 210. 44. 126. 23 \ \ c\$”。但是,如果用十六进制编辑器(如 Hex Editor)来修改 Windows \ system 目录下的 msnp32. dll,将“24 56 E8 17”改为“00 56 E8 17”,就可以让这些“\$共享资源”显示出来。尽管如此,这一技巧仍可视作避开资源共享漏洞的一个好方法。

关闭资源共享当然可以完全解决这一问题,但这也中断了共享信息的通讯联接。为此,作者建议用户要根据自己的要求灵活地设置共享信息的属性,如将文件名设置为“\$共享名”,“访问类型”设置为“根据密码访问”或“只读”(加只读密码)。此外,要及时关闭不需要的共享信息。

1.2 资源共享密码漏洞 在 Windows9X/Me/2000 中,资源共享的密码存放在注册表中,具体位置在:HKEY _ LOCAL _ MACHINE \ Software \ Microsoft

\\ Windows \\ CurrentVersion \\ Network \\ LanMan 下。右栏的 ParmLenc 列出的为完全共享密码, Parm2enc 列出的为只读共享密码。目前密码破解公式已广为流传, 用户可以很轻松地破译出共享密码。另外, 在 Windows98 还存在上述另一密码漏洞, 即通过特定动态链接库文件的替换, 用户可以轻松地绕过密码。解决办法是使用 Windows2000 或 windowsXP 操作系统, 并且设法防止他人破解共享密码。

1.3 CONCON 漏洞 该漏洞是 Wind9X 一直未能解决的一个老漏洞。在 Wind9X 中有三个设备驱动程序: ①CON: 输入及输出设备驱动程序, ②NUL: 空设备驱动程序, ③AUX: 辅助设备驱动程序。用户只要运行这三个程序, 就会立即导致系统的死机, 如运行“C: \\ CON \\ CON”或“C: \\ AUX \\ AUX”等。更重要的是, 在网络环境下该漏洞可以通过资源共享来远程执行, 如运行“\\ \\ 210. 44. 126. 23 \\ D \\ CON \\ CON”(其中“\\ \\ 210. 44. 126. 23”为对方的 IP, D 为对方的共享盘符)。

解决办法为: ①将系统升级至 WindowsMe、Windows2000 或 WindowsXP, ②下载安装补丁程序 conconfix 并添加到“启动”组, ③安装网络防火墙。

1.4 IP 漏洞 在网络环境下用户很难隐藏本机的 IP, 但可轻而易举地探到对方的 IP, 如可以通过运行 Winipcfg 知道本机 IP, 也可以利用网络防火墙 SkyNet、TraceIP 或 IPTools 等工具探查对方的 IP。

目前针对于 IP 的攻击程序已有很多个版本。这类攻击工具主要利用 Windows95/NT 下 NetBios 网络协议的例行处

理程序 OOB 的漏洞, 将一个资料封包以 OOB 方式放在某 IP 地址的某个开启的端口上(通常为 139、138、137、113 等端口), 造成突然死机。遭受此类攻击的对象主要是采用 Windows95 操作系统的工作用机。Windows98 操作系统在这方面的防御能力有所加强。如果安装的是 Windows95 操作系统, 可以通过修改注册表 HKEY _ LOCAL _ MACHINE \\ System \\ Current Control Set \\ Services \\ VxD \\ MSTCP, 新建字符串值“BSDU rgeNT”, 将此键值设置为“0”, 并将 Windows \\ System 目录中的 Vnbt. 386 更名为 Vnbt. bak 来防范攻击。为了更有效地防止 IP 炸弹的攻击, 建议安装网络防火墙。

2 当前流行的网络病毒及其防护措施

随着网络在社会各个领域的普及和推广, 通过网络传播的计算机病毒亦日益猖獗起来, 并成为病毒主流。病毒从 1983 年诞生以来, 数量一直呈巨增状态, 目前大约有 5~6 万种病毒。其中 SirCam(齿轮先生)、WantJob(求职信)、FunLove(欢爱)、HappyTime(欢乐时光)、CodeRed2(红色代码 II)、Magistr(马吉斯特)、VBS. Sst(库尔尼科娃)、VBS. homepage 和 Navidad. B 被列为 2001 年度十大危害病毒。目前发现新的病毒或病毒变种在不断萌生, 随时都在威胁着图书馆工作用机的安全。

2.1 宏病毒 由于微软的 office 系列办公软件和 Windows 系统占据了绝大多数 PC 软件市场, 加上 Windows 和 office 提供了宏病毒编制和运行所必需的库支持和传播机会, 所以宏病毒是最容易编制和流传

的病毒之一。目前宏病毒更多地感染 Word 文档。在 Word 打开感染病毒的文档时,宏病毒会接管计算机,并将自己感染到其他文档,或直接删除文件等。Word 将宏和其他样式储存在模板中,因此宏病毒总是把文档转成模板再储存它们的宏。宏病毒在发作的时候没有特别的迹象,通常是会伪装成其他的待于确认的对话框。感染了宏病毒后,会出现文件不能打印、Office 文档无法保存或另存为等症状。更为严重的是,宏病毒发作时会删除硬盘上的文件,将非公开的文件复制到公开场合,或从硬盘上将文件发送到 E-mail、FTP 地址等。

防止该病毒办法是,尽量避免多人共用一套 office 办公系统,并且要加载病毒实时监控程序。另外,该病毒的变种可以附带在邮件的附件里,因此在打开邮件或预览邮件时应该加以小心。令人欣慰的是,目前流行的各种杀毒软件基本都可以清除这类病毒。

2.2 CIH 病毒 CIH 是本世纪最著名和最有破坏力的病毒之一,也是第一个能破坏硬件的病毒。该病毒主要是通过篡改 BIOS 数据,造成计算机开机就黑屏,从而让用户无法进行任何数据抢救和杀毒操作。CIH 的变种能在网络上通过捆绑其他程序或是邮件附件传播,并且常常删除硬盘上的文件及破坏硬盘的分区表。因此,CIH 发作以后,硬盘数据挽回的可能性非常小。

目前已有 CIH 免疫程序诞生了,包括病毒制作者本人写的免疫程序。一般运行了免疫程序就可以有效地防护 CIH 了。

如果已经中毒,但尚未发作,记得先备份硬盘分区表和引导区数据,再进行查杀,以免杀毒失败造成硬盘无法自举。

2.3 蠕虫病毒 以尽量多复制自身而得名,多感染电脑和占用系统、网络资源,使 PC 和服务器因负荷过重而死机,并以使系统内数据混乱为主要的破坏方式。它不一定马上删除磁盘文件,如爱虫病毒和尼姆达病毒。目前对于这类病毒已有专门的查杀工具。

2.4 木马病毒 木马病毒源自古希腊特洛伊战争中著名的“木马计”而得名。特洛伊木马程序是黑客常用的攻击工具,其隐蔽性、伪装性很强,很难防范。它可以通过资源共享漏洞、微软的 IIS 漏洞、电子信箱、随意地下载文件、甚至只是打开了一个网页感染系统,在远程计算机的系统中植入一个能够在 Windows 启动时自动运行的程序,采用服务器或客户机的运行方式控制远程计算机。黑客可以借此窃取口令、浏览驱动器、修改文件、登录注册表等。

对于上述各种病毒防护办法是除了安装病毒防火墙、网络防火墙外,再安装专用的木马查杀软件,如 Trojan Hunter(木马猎人)或 Trojan Remover(木马清道夫)等。建议及时升级杀毒软件,并定期检查系统是否感染病毒或木马。□

参考文献

- 1 王纪英.图书馆阅览室网络的构建及优化方案刍议.贵图季刊,2001(4)
- 2 鲁士文等.计算机通信网络.北京:科学出版社,2000

(收稿日期:2002-05-10)