两招填补Windows2003D 服务器漏洞 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/264/2021_2022__E4_B8_A4_E6_8B_9B_E5_A1_AB_E8_c67_264851.htm DNS 是域名系统 (Domain Name System) 的缩写。大家在上网时输入的网址，是通过域名解析系解析找到相对应的IP地址才能访问到网站。但是最近微软的Windows 2000和Windows 2003的DNS服务出现一个极高的安全漏洞，如果被黑客成功利用的话，那么我们的上网操作将遇到巨大的麻烦。 黑客姓名：张均诚 黑客特长：Windows系统漏洞研究 使用工具：DNS服务器漏洞利用工具 黑客自白：最近Windows系统的DNS出现了0day漏洞，自从这个安全漏洞的代码被披露，攻击这个漏洞的Nirbot蠕虫已经出现了各种变体。如果这个漏洞被黑客利用，那么系统就会被黑客完全控制。 DNS漏洞打开系统防线 Windows DNS如果存在这个漏洞，那么它在工作时，RPC接口如果处理到有非常规的畸形连接请求，就会向外释放管理员权限，让黑客可以利用这种漏洞完全控制系统。黑客可以通过向有这个漏洞的系统发送一个经过特别设计的RPC数据包，就能够获得该系统的管理员权限，远程执行任意指令。 小知识：什么是RPC 远程过程调用 (RPC) 是一种协议，程序可使用这种协议向网络中的另一台计算机上的程序请求服务。由于使用 RPC 的程序不必了解支持通信的网络协议的情况，因此 RPC 提高了程序的互操作性。 此前，RPC中也出现过数个漏洞，其中包括导致Blaster蠕虫大爆发的那个漏洞。这一最新的漏洞是一个堆栈溢出漏洞，给微软和Windows用户带来了很大麻烦。 根据微软发布的消息，Windows XP和Windows Vista不会

受到这一DNS漏洞的影响，Windows 2000 Server SP4、Windows Server 2003 SP1、Windows Server 2003 SP2则存在这一漏洞。 轻松利用DNS漏洞 打开系统的命令提示符，接着跳转到DNS服务器漏洞利用工具所在的命令，然后执行该漏洞利用工具(图1)。 在该漏洞的利用程序中执行命令：dns.exe -h 127.0.0.1 -t 1 -p 445，因为我是在本地计算机上进行测试的，所以其中的IP地址为127.0.0.1，而且需要根据服务器版的语言设置参数。当利用工具提示溢出成功以后，就可以利用telnet命令或程序nc连接存在漏洞的服务器中的4444端口，比如telnet 127.0.0.1 4444(图2)。需要说明的是，该工具的成功率并不是特别的高，所以在测试的时候需要多进行几次 