# 内网域内信息收集

## 查询权限

查看当前权限命令如下

```
whoami
```

获取台主机的权限后,有三种情况:

1、本地普通用户:当前为本机的user用户


2、本地管理员用户:当前为本机的admmistrator


3、域内用户:当前为域内普通用户


4、域内用户:当前为hacke域内的administrator用户


在这四种情况中。

- 如果当前内网中存在域,那么本地普通用户只能查询本机相关信息,不能查询域内信息.
- 而本地管理员用户和域内用户可以查询域内信息.

其原理是:域内的所有查询都是通过域控制器实现的（基于LDAP协议）,而这个查询需要经过权限认证,所以,只有域用户才拥有这个权限;当域用户执行查询命令时,会自动使用Kerberos协议进行认证,无须额外输人账 号和密码

本地管理员Admmistrator权限可以直接提升为Ntauthority或System权限,因此,在域中,除普通用户外,所有的机器都有一个机器用户（用户名是机器名加上"$"）。在本质上,机器的system用户对应的就是域里面的机器用户所以,使用System权限可以运行域内的查询命令。

## 判断域的存在

获得了本机的相关信息后'就要判断当前内网中是否存在域°如果当前内网中存在域,就需要判断所控主机是否在域内°下面讲解几种方法。

## 1、Ipconfig /all命令

执行命令,可以查看网关IP地址、DNS的IP地址,域名、本机是否和DNS服务器处于同一网段等信息

```
C:\>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : PC-2008
   主 DNS 后缀 . . . . . . . . . . . : hack.com
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : hack.com
```

然后,通过反向解析查询命令nslookup来解析域名的IP地址。用解析得到的IP地址进行对比判断域控制器和DNS服务器是否在同一台服务器上。

```
C:\>nslookup hack.com
服务器:  UnKnown
Address:  192.168.41.10

名称:    hack.com
Address:  192.168.41.10
```

## 2、SystemInfo

执行如下命令,"域"即域名,登录服务器"为域控制器°如果"域'为"WORKGROUP",表示当前服务器不在域内

```
C:\>SystemInfo | findstr "域"
系统区域设置:     zh-cn;中文(中国)                                a
输入法区域设置:   zh-cn;中文(中国)
域:               hack.com
```

## 3、net config workstation

```
C:\>net config workstation
计算机名                     \\PC-2008
计算机全名                   PC-2008.hack.com
用户名                       bob

工作站正运行于
        NetBT_Tcpip_{B942733B-03AC-4053-9F29-E84AE5F5553E} (000C29D4E2A4)

软件版本                     Windows Server 2008 HPC Edition

工作站域                     HACK
工作站域 DNS 名称            hack.com
登录域                       HACK

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。
```

## 4、Net time /domain

一般会有如下三种情况:

1.存在域，但当前用户不是域用户

```
C:\>net time /domain
发生系统错误 5。

拒绝访问。
```

2.存在域，并且当前用户是域用户

```
C:\>Net time /domain
\\DC.hack.com 的当前时间是 2022/3/31 13:53:21

命令成功完成。
```

3.当前网络环境为工作组，不存在域

```
C:\Users\Administrator>net time /domain
找不到域 BM 的域控制器。

请键入 NET HELPMSG 3913 以获得更多的帮助。
```

# 域内基础信息

确定了当前内网拥有的域,且所控制的主机在域内,就可以进行域内相关信息的收集了。介绍的查询命令在本质上都是通过LDAP协议到域控制器上进行查询的,所以在查询 时需要进行权限认证。只有域用户才拥有此权限,本地用户无法运行本节介绍的查询命令( System 权限用户除外。在域中,除普通用户外,所有的机器都有一个机器用户,其用户名为机器名加上 "$"。 System权限用户对应的就是域里面的机器用户,所以System权限用户可以运行本节介绍 的查询命令)

## 1、查询域

查询域的命令如下

如果出现"此工作组的服务器列表当前无法使用" 开启服务：Server ， WorkStation，computer Browser,关闭防火墙

```
net view /domain
```

```
C:\>net view /domain
Domain

---------------------------------------------------------------------------
HACK
命令成功完成。
```

## 2、查询域内所有计算机

```
net view/domain:域名
```

```
C:\>net view /domain:hack
服务器名称            注解

-------------------------------------------------------------------------------
\\DC
\\PC-2003              ping
命令成功完成。
```

执行如下命令,就可以通过查询得到的主机名对主机角色进行初步判断,如图。例如,"dev"可能是开发服务器,"web""app"可能是Web服务器,"NAS"可能是存储服务器" fileserver"可能是文件服务器等。

## 3、查询域内所有用户组列表

```
net group /domain
```

```
C:\>net group /domain
这项请求将在域 hack.com 的域控制器处理。


\\DC.hack.com 的组帐户

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Protected Users
*Read-only Domain Controllers
*Schema Admins
命令成功完成。
```

执行如下命令,查询域内所有用户组列表。

系统自带的常见用户身份如下:

```
DomainAdmins:域管理员。
DomainComputers:域内机器。
DomainControllers:域控制器。
DomainGusers:域访客,权限较低。
DomainUser:域用户。
EnterpriseAdmins:企业系统管理员用户
在默认情况下, Domain admins和Enterprise Admins对域内所有域控制器有完全控制权限
```

## 4、查询所有域成员计算机列表

执行如下命令，查询所有域成员计算机列表

```
net group "domain computers" /domain
```

```
C:\>net group "domain computers" /domain
这项请求将在域 hack.com 的域控制器处理。

组名     Domain Computers
注释     加入到域中的所有工作站和服务器

成员

-------------------------------------------------------------------------------
PC-2008$
命令成功完成。
```

## 5、获取域密码信息

执行如下命令'获取域密码策略、密码长度、错误锁定等信息

```
net accounts /domain
```

```
C:\>net accounts /domain
这项请求将在域 hack.com 的域控制器处理。

强制用户在时间到期之后多久必须注销?:     从不
密码最短使用期限(天):                   1
密码最长使用期限(天):                   42
密码长度最小值:                         7
保持的密码历史记录长度:                 24
锁定阈值:                               从不
锁定持续时间(分):                       30
锁定观测窗口(分):                       30
计算机角色:                             PRIMARY
命令成功完成。
```

## 6、获取域信任信息

执行如下命令'获取域信任信息

```
nltest /domain_trusts
```

```
C:\>nltest /domain_trusts
域信任的列表:
    0: HACK hack.com (NT 5) (Forest Tree Root) (Primary Domain) (Native)
此命令成功完成
```

# 查找域控主机

## 1、查看域控制器的机器名

执行如下命令,可以看到,域控制器的机器名

```
nltest /DCLIST:hack
```

```
C:\>nltest /DCLIST:hack
获得域“hack”中 DC 的列表(从“\\DC”中)。
    DC.hack.com [PDC]  [DS] 站点: Default-First-Site-Name
此命令成功完成
```

## 2、查看域控制器的主机名

执行如下命令,可以看到,域控制器的主机名

```
nslookup -type=SRV _ldap._tcp
```

```
C:\>nslookup -type=SRV _ldap._tcp
服务器:  UnKnown
Address:  192.168.41.10

_ldap._tcp.hack.com     SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = dc.hack.com
dc.hack.com     internet address = 192.168.41.10
```

## 3、查看当前时间

在通常情况下,时间服务器为主域控制器。执行如下命令

```
net time /domain
```

```
C:\>net time /domain
\\DC.hack.com 的当前时间是 2022/3/31 15:26:36

命令成功完成。
```

## 4、查看域控制器组

执行如下命令,查看域控制器组。,其中有一台机器名为"DC"的域控制器`

```
net group "Domain Controllers" /domain
```

```
C:\>net group "Domain Controllers" /domain
这项请求将在域 hack.com 的域控制器处理。

组名     Domain Controllers
注释     域中所有域控制器

成员

-------------------------------------------------------------------------------
DC$
命令成功完成。
```

在实际网络中,一个域内一般存在两台或两台以上的域控制器,其目的是:一旦主域控制器发生故障,备用的域控制器可以保证域内的服务和验证工作正常进行。

# 获取域内用户

## 1、向域控制器进行查询

执行如下命令,向域控制器DC进行查询,,域内有多个用户。其中,krbtgt 用户不仅可以创建票据授权服务(TGS)的加密密钥,还可以实现多种域内权限持久化方法,

```
net user /domain
```

```
C:\>net user /domain
这项请求将在域 hack.com 的域控制器处理。


\\DC.hack.com 的用户帐户

-------------------------------------------------------------------------------
Administrator            bob                      Guest
jack                     krbtgt
命令成功完成。
```

## 2、获取域内用户的详细信息

执行如下命令,可以获取域内用户的详细常见参数包括用户名、描述信息、SID、域名、状态等。

```
wmic useraccount get/all
```

```
C:\>wmic useraccount get/all
AccountType  Caption               Description                    Disabled  Domain   FullName  InstallDate  LocalAccount  Lockout  Name           PasswordChangeable  PasswordExpires  P
uired  SID                                          SIDType  Status
512          PC-2008\Administrator  管理计算机(域)的内置帐户           FALSE     PC-2008                         TRUE          FALSE    Administrator  TRUE                TRUE             T
       S-1-5-21-3432382454-1205603526-922924321-500  1        OK
512          PC-2008\Guest          供来宾访问计算机或访问域的内置帐户  TRUE      PC-2008                         TRUE          FALSE    Guest          FALSE               FALSE            F
       S-1-5-21-3432382454-1205603526-922924321-501  1        Degraded
512          PC-2008\zhangsan       zhangsan                       FALSE     PC-2008  zhangsan                TRUE          FALSE    zhangsan       TRUE                TRUE             T
       S-1-5-21-3432382454-1205603526-922924321-1006 1        OK
512          HACK\Administrator     管理计算机(域)的内置帐户           FALSE     HACK                            FALSE         FALSE    Administrator  TRUE                TRUE             T
       S-1-5-21-2716900768-72748719-3475352185-500   1        OK
512          HACK\Guest             供来宾访问计算机或访问域的内置帐户  TRUE      HACK                            FALSE         FALSE    Guest          FALSE               FALSE            F
       S-1-5-21-2716900768-72748719-3475352185-501   1        Degraded
512          HACK\krbtgt            密钥发行中心服务帐户               TRUE      HACK                            FALSE         FALSE    krbtgt         TRUE                TRUE             T
       S-1-5-21-2716900768-72748719-3475352185-502   1        Degraded
512          HACK\bob                                            FALSE     HACK     bob                     FALSE         FALSE    bob            TRUE                FALSE            T
       S-1-5-21-2716900768-72748719-3475352185-1105  1        OK
512          HACK\jack                                           FALSE     HACK     jack                    FALSE         FALSE    jack           TRUE                FALSE            T
       S-1-5-21-2716900768-72748719-3475352185-1107  1        OK
```

## 3、查看存在的用户

执行如下命令,可以看到,域内用户（server机器有这个命令）

```
dsquery user
```

```
C:\>dsquery user
"CN=Administrator,CN=Users,DC=hack,DC=com"
"CN=Guest,CN=Users,DC=hack,DC=com"
"CN=krbtgt,CN=Users,DC=hack,DC=com"
"CN=bob,CN=Users,DC=hack,DC=com"
"CN=jack,CN=Users,DC=hack,DC=com"
```

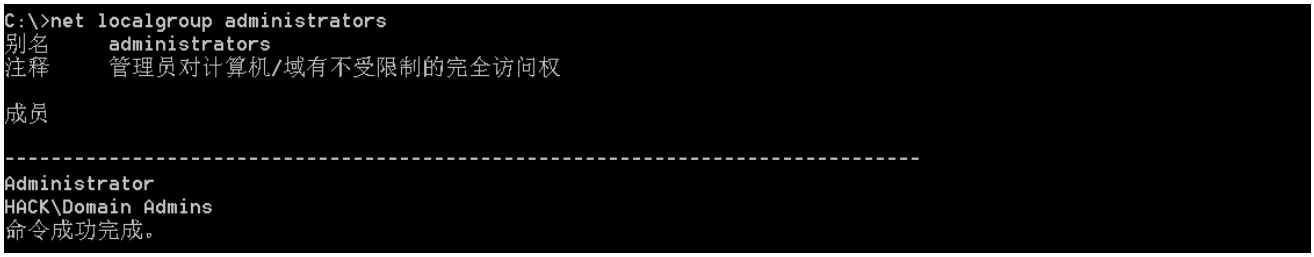
常用的 dsquery命令：

```
dsquery computer        -查找目录中的计算
dsquery contact         -查找目录中的职系人
asquery subnet          -目录中的子网
dsquery group           -查找目录中的组,
dsquery ou              -查找目录中的组织单位,
dsquery site            -最找目景中的站成
dsquery server          -查找目录中的ADDC/LDs实例
asquery user            -查找目录中的用户
dsquery quota           -查找目录中的配颗机定
dsquery partition       -查找目录中的分区
```

## 4、查询本地管理员组用户

```
net localgroup administrators
```

Domain admin组中的用户默认为域内机器的本地管理员用户 在实际应用中'为了方便管 理'会有域用户被设置为域机器的本地管理员用户°




# 查找域管理员

# 查找域管理进程