获取域内用户

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
```

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命令详解

```
ALIAS                   - 对本地系统上可用别名的访问
BASEBOARD               - 基板(也称为主板或系统板)管理。
BIOS                    - 基本输入/输出服务(BIOS)管理。
BOOTCONFIG              - 启动配置管理。
CDROM                   - CD-ROM 管理。
COMPUTERSYSTEM          - 计算机系统管理。
CPU                     - CPU 管理。
CSPRODUCT               - SMBIOS 中的计算机系统产品信息。
DATAFILE                - 数据文件管理。
DCOMAPP                 - DCOM 应用程序管理。
DESKTOP                 - 用户的桌面管理。
DESKTOPMONITOR          - 桌面监视器管理。
DEVICEMEMORYADDRESS     - 设备内存地址管理。
DISKDRIVE               - 物理磁盘驱动器管理。
DISKQUOTA               - 用于 NTFS 卷的磁盘空间使用量。
DMACHANNEL              - 直接内存访问(DMA)通道管理。
ENVIRONMENT             - 系统环境设置管理。
FSDIR                   - 文件系统目录项管理。
GROUP                   - 组帐户管理。
IDECONTROLLER           - IDE 控制器管理。
IRQ                     - 中断请求线路(IRQ)管理。
JOB                     - 提供对使用计划服务安排的作业的访问。
LOADORDER               - 定义执行依赖关系的系统服务的管理。

LOGICALDISK             - 本地存储设备管理。
```

```
LOGON                   - 登录会话。
MEMCACHE                - 缓存内存管理。
MEMORYCHIP              - 内存芯片信息。
MEMPHYSICAL             - 计算机系统的物理内存管理。
NETCLIENT               - 网络客户端管理。
NETLOGIN                - 网络登录信息(属于特定用户)管理。
NETPROTOCOL             - 协议(及其网络特征)管理。
NETUSE                  - 活动网络连接管理。
NIC                     - 网络接口控制器(NIC)管理。
NICCONFIG               - 网络适配器管理。
NTDOMAIN                - NT 域管理。
NTEVENT                 - NT 事件日志中的项目。
NTEVENTLOG              - NT 事件日志文件管理。
ONBOARDDEVICE           - 主板(系统板)中内置的通用适配器设备的管理。
OS                      - 已安装操作系统的管理。
PAGEFILE                - 虚拟内存文件交换管理。
PAGEFILESET             - 页面文件设置管理。
PARTITION               - 物理磁盘的已分区区域的管理。
PORT                    - I/O 端口管理。
PORTCONNECTOR           - 物理连接端口管理。
PRINTER                 - 打印机设备管理。
PRINTERCONFIG           - 打印机设备配置管理。
PRINTJOB                - 打印作业管理。
PROCESS                 - 进程管理。
PRODUCT                 - 安装程序包任务管理。
QFE                     - 快速修复工程。
QUOTASETTING            - 卷上的磁盘配额设置信息。
RDACCOUNT               - 远程桌面连接权限管理。
RDNIC                   - 对特定网络适配器的远程桌面连接管理。
RDPERMISSIONS           - 特定远程桌面连接的权限。
RDTOGGLE                - 远程打开或关闭远程桌面侦听程序。
RECOVEROS               - 操作系统出现故障时将从内存收集的信息。
REGISTRY                - 计算机系统注册表管理。
SCSICONTROLLER          - SCSI 控制器管理。
SERVER                  - 服务器信息管理。
SERVICE                 - 服务应用程序管理。
SHADOWCOPY              - 卷影副本管理。
SHADOWSTORAGE           - 卷影副本存储区域管理。
SHARE                   - 共享资源管理。
SOFTWAREELEMENT         - 系统上安装的软件产品元素的管理。
SOFTWAREFEATURE         - SoftwareElement 的软件产品子集的管理。
SOUNDDEV                - 声音设备管理。
STARTUP                 - 当用户登录到计算机系统时自动运行的命令的管理。
SYSACCOUNT              - 系统帐户管理。
SYSDRIVER               - 基本服务的系统驱动程序管理。
SYSTEMENCLOSURE         - 物理系统外壳管理。
SYSTEMSLOT              - 物理连接点(包括端口、插槽和外设以及专用连接点)的管理。
TAPEDRIVE               - 磁带驱动器管理。
TEMPERATURE             - 温度传感器(电子温度计)数据管理。
TIMEZONE                - 时区数据管理。
UPS                     - 不间断电源(UPS)管理。
USERACCOUNT             - 用户帐户管理。

VOLTAGE                 - 电压传感器(电子电压表)数据管理。
```

```
VOLUME                  - 本地存储卷管理。
VOLUMEQUOTASETTING      - 将磁盘配额设置与特定磁盘卷相关联。
VOLUMEUSERQUOTA         - 每用户存储卷配额管理。
WMISET                  - WMI 服务操作参数管理。
```

```
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
```

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
dsquery 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
```

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°

```
C:\>net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------------------
Administrator
HACK\Domain Admins
命令成功完成。
```

查询域管理用户

```
net group "domain admins" /domain
```

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

组名     Domain Admins
注释     指定的域管理员

成员

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

查询域管理员用户组

```
net group "Enterprise Admins" /domain
```

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

组名     Enterprise Admins
注释     企业的指定系统管理员

成员

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