域内基础信息收集

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

```
C:\>whoami
pc-2008\zhangsan
```

2、本地管理员用户:当前为本机的admmistrator

```
C:\>whoami
pc-2008\administrator
```

3、域内用户:当前为域内普通用户

```
C:\Users\bob>whoami
hack\bob

C:\Users\bob>
```

4、域内用户:当前为hacke域内的administrator用户

```
C:\>whoami
hack\administrator
```

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。
```

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)

NET命令详解

NET命令是一个命令行命令，Net命令有很多函数用于实用和核查计算机之间的NetBIOS连接，可以查看我们的管理网络环境、服务、用户、登陆等信息内容；要想获得Net 的HELP可以(1)在Windows下可以用图形的方式，开始->帮助->索引->输入NET；(2)在COMMAND下可以用字符方式：NET /?或NET或NET HELP取得相应的方法的帮助。所有Net命令接受选项/yes和/no(可缩写为/y和/n)。

主要命令				
NET View	NET User	NET Use	NET Time	Net Start
Net Pause	Net Continue	NET Stop	Net Statistics	Net Share
Net Session	Net Send	Net Print	Net Name	Net Localgroup
Net Group	Net File	Net Config	Net Computer	Net Accounts

Net View

```
作用：显示域列表、计算机列表或指定计算机的共享资源列表。
命令格式：`Net view [\\computername | /domain[:domainname]]`
有关参数说明：
     - 键入不带参数的`net view`显示当前域的计算机列表
     - `\\computername` 指定要查看其共享资源的计算机
     - `/domain[:domainname]`指定要查看其可用计算机的域
例如：Net view \\GHQ查看GHQ计算机的共享资源列表。
      Net view /domain:XYZ 查看XYZ域中的机器列表。
```

Net User

作用：添加或更改用户帐号或显示用户帐号信息。
命令格式：`Net user [username [password | *] [options]] [/domain]`
有关参数说明：
- 键入不带参数的Net user查看计算机上的用户帐号列表
- username添加、删除、更改或查看用户帐号名
- password为用户帐号分配或更改密码
- 提示输入密码
- `/domain`在计算机主域的主域控制器中执行操作。该参数仅在Windows NT Server 域成员的 Windows NT Workstation 计算机上可用。默认情况下，Windows NT Server 计算机在主域控制器中执行操作。注意：在计算机主域的主域控制器发生该动作。它可能不是登录域。例如：`Net user ghq123`查看用户GHQ123的信息。

Net Use 作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：`Net use [devicename | *] [\\computername\sharename[\volume]] no}]]` password|*] [[/delete]| [/persistent:{yes |
有关参数说明：
- 键入不带参数的Net use列出网络连接
- devicename指定要连接到的资源名称或要断开的设备名称
- `\\computername\sharename`服务器及共享资源的名称
- password访问共享资源的密码
- *提示键入密码
- `/user`指定进行连接的另外一个用户
- `domainname`指定另一个域
- `username`指定登录的用户名
- `/home`将用户连接到其宿主目录
- `/delete`取消指定网络连接
- `/persistent`控制永久网络连接的使用。
例如：`Net use f: \\GHQ\TEMP` 将\GHQ\TEMP目录建立为F盘
`Net use f: \GHQ\TEMP` /delete 断开连接。

Net Time 作用：使计算机的时钟与另一台计算机或域的时间同步。

命令格式：`Net time [\\computername | /domain[:name]] [/set]`
有关参数说明：
- `\\computername`要检查或同步的服务器名
-`/domain[:name]`指定要与其时间同步的域
- `/set`使本计算机时钟与指定计算机或域的时钟同步。

Net Start 作用：启动服务，或显示已启动服务的列表。

命令格式：`Net start service`

Net Pause 作 用：暂停正在运行的服务。

命令格式：`Net pause service`

Net Continue 作用：重新激活挂起的服务。

命令格式：`Net continue service`

Net Stop 作用：停止 Windows NT/2000/2003 网络服务。

```
命令格式：`Net stop service`
下面我们来看看上面四条命令里服务包含哪些服务：
```

9.Net Statistics 作用：显示本地工作站或服务器服务的统计记录。

```
命令格式：`Net statistics [workstation | server]`
有关参数说明：
·键入不带参数的Net statistics列出其统计信息可用的运行服务
·`workstation`显示本地工作站服务的统计信息
·`server`显示本地服务器服务的统计信息
例如：Net statistics server | more显示服务器服务的统计信息。
```

10.Net Share 作用：创建、删除或显示共享资源。

```
命令格式：`Net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]`
有关参数说明：
· 键入不带参数的Net share显示本地计算机上所有共享资源的信息
· `sharename`是共享资源的网络名称
· `drive:path`指定共享目录的绝对路径
· `/users:number`设置可同时访问共享资源的最大用户数
· `/unlimited`不限制同时访问共享资源的用户数
· `/remark:"text "`添加关于资源的注释，注释文字用引号引住
例如： `Net share yesky=c:\temp /remark:"my first share"`
以yesky为共享名共享C:\temp
`Net share yesky /delete`停止共享yesky目录
```

Net Session 作用：列出或断开本地计算机和与之连接的客户端的会话。

```
命令格式：`Net session [\\computername] [/delete]`
有关参数说明：
·键入不带参数的Net session显示所有与本地计算机的会话的信息。
·`\\computername`标识要列出或断开会话的计算机。
·`/delete`结束与 `\computername` 计算机会话并关闭本次会话期间计算机的所有打开文件。如果省略
`\computername` 参数，将取消与本地计算机的所有会话。
例如：`Net session [url=file://\\GHQ]\\GHQ[/url]`要显示计算机名为GHQ的客户端会话信息列表。
```

Net Send 作用：向网络的其他用户、计算机或通信名发送消息。

```
命令格式：`Net send {name | * | /domain[:name] | /users} message`
有关参数说明：
·`name`要接收发送消息的用户名、计算机名或通信名
·* 将消息发送到组中所有名称
·`/domain[:name]`将消息发送到计算机域中的所有名称
·`/users`将消息发送到与服务器连接的所有用户
·`message`作为消息发送的文本
例如：`Net send /users server will shutdown in 10 minutes`.给所有连接到服务器的用户发送消息。
```

Net Print 作用：显示或控制打印作业及打印队列。

命令格式：`Net print [\\computername ] job# [/hold | /release | /delete]`
有关参数说明：
·`computername`共享打印机队列的计算机名
·`sharename`打印队列名称
·`job#`在打印机队列中分配给打印作业的标识号
·`/hold`使用`job#`时，在打印机队列中使打印作业等待
·`/release`释放保留的打印作业
·`/delete`从打印机队列中删除打印作业
例如：`Net print \\GHQ\HP8000列出[url=file://\\GHQ]\\GHQ[/url]`计算机上HP8000打印机队列的目录。

Net Name 作用：添加或删除消息名（有时也称别名），或显示计算机接收消息的名称列表。

命令格式：`Net name [name [/add | /delete]]`
有关参数说明：
·键入不带参数的Net name列出当前使用的名称
·`name`指定接收消息的名称
·`/add`将名称添加到计算机中
·`/delete`从计算机中删除名称

Net Localgroup 作 用：添加、显示或更改本地组。

命令格式：`Net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]`
有关参数说明：
·键入不带参数的`Net localgroup`显示服务器名称和计算机的本地组名称
·`groupname`要添加、扩充或删除的本地组名称
·`/comment: "text "`为新建或现有组添加注释
·`/domain`在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作
·`name [ ...]`列出要添加到本地组或从本地组中删除的一个或多个用户名或组名
·`/add`将全局组名或用户名添加到本地组中
·`/delete`从本地组中删除组名或用户名
例如：`Net localgroup ggg /add` 将名为ggg的本地组添加到本地用户帐号数据库；
`Net localgroup ggg` 显示ggg本地组中的用户。

Net Group 作 用：在 Windows NT/2000/2003 Server 域中添加、显示或更改全局组。

命令格式：`Net group groupname {/add [/comment:"text "] | /delete} [/domain]`
有关参数说明：
·键入不带参数的Net group显示服务器名称及服务器的组名称
·`groupname`要添加、扩展或删除的组
·`/comment:"text "`为新建组或现有组添加注释
·`/domain`在当前域的主域控制器中执行该操作，否则在本地计算机上执行操作
·`username[ ...]`列表显示要添加到组或从组中删除的一个或多个用户
·`/add`添加组或在组中添加用户名
·`/delete`删除组或从组中删除用户名
例如：`Net group ggg GHQ1 GHQ2 /add`将现有用户帐号GHQ1和GHQ2添加到本地计算机的ggg组。

Net File 作用：显示某服务器上所有打开的共享文件名及锁定文件数。

```
    命令格式：`Net file [id [/close]]`
    有关参数说明：
    ·键入不带参数的Net file获得服务器上打开文件的列表
    ·`id`文件标识号
    ·/close关闭打开的文件并释放锁定记录
```

Net Config 作用：显示当前运行的可配置服务，或显示并更改某项服务的设置。

```
 命令格式：`Net config [service [options]]`
有关参数说明：
·键入不带参数的Net config显示可配置服务的列表
·`service`通过Net config命令进行配置的服务(server或workstation)
`options`服务的特定选项
```

Net Computer 作用：从域数据库中添加或删除计算机

```
命令格式：Net computer \computername {/add | /del}
有关参数说明：
       ·\\computername指定要添加到域或从域中删除的计算机
       ·/add将指定计算机添加到域
       ·/del将指定计算机从域中删除
       例如：Net computer \\js /add将计算机js 添加到登录域。
```

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。
```

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。

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
```

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。
```

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。
```

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
```