定位域管理员

在内网中，通常会部署大址的网络安全系统和设备,例如IDS、IPS、日志审计、安全网关、 反病毒软件等。在域网络攻击测试中,获取域内的一个支点后，需要获取域管理员权限. 在一个域中，当计算机加入域后，会默认给域管理员组赋予本地系统管理员权限,也就是说, 当目机被添加到城中.成为域的成员主机后，系统会自动将域管理员组添加到本地系统管理员组中，因此域管理员组的成员都可以访问本地计算机，且具备安全控制权限

定位域内管理员的常规果道，一是日志，二是会话。日志是指本地机器的管理员日志，会话是指域内每台机器的登录会话

假设已经在Windows域中取得了普通用户权限，希望在城内横向移动，需 要知道域内用户登录的位置、他是否是任何系统的本地管理员、他所属的组、他是否有权访问文 件共享等。枚举主机、用户和组，有助于更好地了解域的布局。

手动定位域管理员

```
net view /domain 查看当前域名
net view /domain:域名 查看域内部所有计算机名
net group /domain 查看域内部所有用户组列表
net group "domain computers" /domain 查看所有域成员计算机列表
net accounts /domain 查看域密码信息
nltest /domian_trusts 获取域信任信息
nltest /DCLIST:域名 查看域控制器机器名
net time /domain 查看当前时间，因为时间服务器也是主域服务器，可以看到域服务器的机器名
net group "Domain Controllers" /domain 查看域控制器组，因为可能有不止一台域控，有主备之分
net user /domain 查询域内用户，会看到熟悉的krbtgt用户
wmic useraccount get /all 获取域内用户详细信息
dsquery user 查看域内存在的用户
net localgroup administrators 查看本地管理员用户组
net group "domain admins" /domain 查询域管理员用户
```

psloggedom.exe工具

psloggedon.exe 可以显示本地登录的用户和通过本地计算机或远程计算机的资源登录的用户。如果指定了用户名而不是计算 机，psloggedon.exe 会搜索网络邻居中的计算机，并显示该用户当前是否已登录。

```
psloggedon.exe [-] [-l] [-x] [\\computername或username]
```

```
C:\Users\zs\Desktop>PsLoggedon.exe \\PC-2003

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     <unknown time>             HACK\ls

Users logged on via resource shares:
     2022/5/27 1:15:23          HACK\ZS
```

```
C:\Users\zs\Desktop>PsLoggedon.exe zs

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

HACK\zs logged onto DC remotely.
HACK\zs logged onto PC-2003 remotely.
HACK\zs logged onto PC-2008 locally.
HACK\zs logged onto PC-2008 remotely.
```

PVEDFindADUser.exe工具

pveFindADUser.exe 可用于查找 Active Directory 用户登录的位置，枚举域用户，以及查找在 特定计算机上登录的用户，包括本地用户、通过RDP 登录的用户、用于运行服务和计划任务的用户账 户。运行该工具的计算机需要具有.NETFramework 2.0，并且需要具有管理员权限

```
-h：显示帮助信息
-current["username"]：如果仅指定-current参数，将获取目标计算机上当前登录的所有用户。如果指定了用户名（Domain\Username），则显示该用户登录的计算机
-last["username"]：如果仅指定-last参数，将获取目标计算机上最后一个登录用户。如果指定了用户名（Domain\Username），则显示此用户上次登录的计算机。根据网络的安全策略，可能会隐藏最后一个登录用户的用户名，此时使用该工具可能无法得到用户名
-noping：阻止该工具在获取用户登陆信息之前对目标执行ping命令
-target：可选参数，用于指定要查询的主机。如果未指定该参数，将查询域中的所有主机。如果指定了此参数，主机名列表由逗号分隔
直接运行"pvefindaduser.exe -current"，即可显示域中所有计算机上当前登录的用户
```

```
C:\Users\administrator.HACK.000\Desktop>PVEFindADUser.exe -current
 ----------------------------------------
  PVE Find AD Users
  Peter Van Eeckhoutte
  (c) 2009 - http://www.corelan.be:8800
  Version : 1.0.0.12
 ----------------------------------------
 [+] Finding currently logged on users ? true
 [+] Finding last logged on users ? false

 [+] Enumerating all computers...
 [+] Number of computers found : 3
 [+] Launching queries
     [+] Processing host : DC.hack.com (Windows Server 2012 R2 Standard)
         - Logged on user : hack\administrator
     [+] Processing host : PC-2008.hack.com (Windows Server 2008 HPC Edition;Ser
vice Pack 1)
         - Logged on user : hack\zs
         - Logged on user : hack\administrator
         - Logged on user : pc-2008\administrator
     [+] Processing host : pc-2003.hack.com (Windows Server 2003;Service Pack 2)

         - Logged on user : hack\ls
 [+] Report written to report.csv
```

netview.exe

netview.exe 是一个枚举工具，使用 WinAPI 枚举系统，利用NetSessionEnum找寻登陆会话，利NetShareEnum找寻共享，利用NetWkstaUserEnum枚举登陆的用户。同时，netview.exe 能够查询共享入口和有价值的用户。netview.exe的绝大部分功能不需要管理员权限就可以使用。

使用语法:
netview.exe <参数>
-h: 显示帮助菜单。
-f filename.txt: 指定从中提取主机列表的文件。
-e filename.txt: 指定要排除的主机名文件。
-o filename.txt: 将所有输出重定向到文件。
-d domain: 指定从中提取主机列表的域。如果没有指定，则使用当前域。
-g group: 指定用户搜寻的组名。如果没有指定，则使用 Domain Admins。
 -c: 检查对已找到共享的访问权限。

```
[+] Host: PC-2003
Enumerating AD Info[+] PC-2003 - Comment - ping
[+] P - OS Version - 5.2

Enumerating IP Info
[+] (null) - IPv4 Address - 127.0.0.1

Enumerating Share Info
[+] PC-2003 - Share : C$                    : ????
[+] PC-2003 - Share : IPC$                  : ?? IPC
[+] PC-2003 - Share : ADMIN$                : ????

Enumerating Session Info
[+] PC-2003 - Session -  from PC-2008 - Active: 0 - Idle: 0
[+] PC-2003 - Session - ADMINISTRATOR from PC-2008 - Active: 0 - Idle: 0

Enumerating Logged-on Users
[+] PC-2003 - Logged-on - HACK\ls
```

NSE脚本

如果存在域账户或者本地账户就可以使用Nmap的smb-enum-sessions.nes引擎获取远程机器的登录会话（不需要管理员权限）。

```
smb-enum-domain：对域控制器进行信息收集，可以获取主机的信息、用户、可使用密码策略的用户等
smb-enum-users：在进行域渗透测试时，如果获得了域内某台主机的权限，无法获取更多的域用户信息，就可以借助这个脚本对域控制器进行扫描
smb-enum-shares：遍历远程主机的共享目录
smb-enum-processes：对主机的系统进行遍历。通过这些信息，可以知道目标主机上正在运行哪些软件。
smb-enum-sessions：获取域内主机的用户登录会话，查看当前是否有用户登录。
smb-os-discovery：收集目标主机的操作系统、计算机名、域名域林名称、NetBIOS机器名、NetBIOS域名，工作组、
```

PowerView脚本

PowerView 脚本中包含了一系列的 powershell 脚本，信息收集相关的脚本有 Invoke-StealthUserHunter、Invoke-UserHunter 等，

```
powershell.exe -exec bypass -command "& { import-module .\PowerView.ps1;Invoke-UserHunter}"
```

```
PS C:\Users\Administrator\Desktop> Invoke-UserHunter


UserDomain      : HACK
UserName        : Administrator
ComputerName    : DC.hack.com
IPAddress       : 192.168.41.10
SessionFrom     :
SessionFromName :
LocalAdmin      :

UserDomain      : PC-2003
UserName        : Administrator
ComputerName    : pc-2003.hack.com
IPAddress       : 192.168.41.30
SessionFrom     :
SessionFromName :
LocalAdmin      :
```