

2.7 收集域内基础信息

确定了当前内网拥有的域,并且所控制的主机在域里面,就可以进行域内相关信息的收集了。因为这些查询命令本质上都是通过 LDAP 协议去域控制器上查询的,查询时候需要经过权限认证,只有域用户才有这个权限,所以本地用户是无法运行以下命令的 (system 权限用户除外。在域里面,除了普通用户,所有机器都有一个机器用户,用户名为机器名加 “\$”。system 用户对应的就是域里面的机器用户,所以 system 权限用户是可以运行以下查询命令的)。

1. 查询域

查询域的命令如下,如图 2-50 所示。

```
net view /domain
```



```
c:\Windows\Temp>net view /domain
Domain

-----
HACKE
WORKGROUP
命令成功完成。
```

图 2-50 查询域

2. 查询此域内所有计算机

执行如下命令，可以通过查询得到的主机名来对主机角色进行初步判断，如图 2-51 所示。例如，“dev”可能是开发服务器，“web”或者 app 可能是 Web 服务，“NAS”可能是存储服务器，“fileserver”可能是文件服务器等。

```
net view /domain:XXX
```

```
c:\Windows\Temp>net view /domain:HACKE
服务器名称      注解
-----
\\DC
\\WIN-2008
命令成功完成。
```

图 2-51 查询此域内的所有计算机

3. 查询域内所有用户组列表

执行如下命令，查询域内所有用户组列表，如图 2-52 所示。

```
net group /domain
```

```
c:\Windows\Temp>net group /domain
这项请求将在域 hacke.testlab 的域控制器处理。

\\DC.hacke.testlab 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。
```

图 2-52 查询域内所有用户组列表

可以看到，该域含有 13 个组。系统自带的常见组如下。



- Domain Admins：域管理员组。
- Domain Computers：域内机器。
- Domain Controllers：域控制器。
- Domain Guest：域访客组，权限较低。
- Domain Users：域用户。
- Enterprise Admins：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，如图 2-53 所示。

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

```
c:\Windows\Temp>net group "domain computers" /domain
这项请求将在域 hacke.testlab 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
成员

-----
WIN-2008$      WIN7-X64-TEST$
命令成功完成。
```

图 2-53 查询所有域成员计算机列表

5. 获取域密码信息

执行如下命令，获得域密码策略设置、密码长短、错误锁定等信息，如图 2-54 所示。

```
net accounts /domain
```

```
c:\Windows\Temp>net accounts /domain
这项请求将在域 hacke.testlab 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。
```

图 2-54 获取域密码信息

6. 获取域信任信息

执行如下命令，获取域信任信息，如图 2-55 所示。

```
nltest /domain_trusts
```

```
c:\Windows\Temp>nltest /domain_trusts
域信任的列表:
    0: HACKE hacke.testlab <NT 5> <Forest Tree Root> <Primary Domain> <Native>
此命令成功完成
```

图 2-55 获取域信任信息

2.8 查找域控制器

1. 查看域内控制器的机器名

执行如下命令，可以看到域控制器机器名为 DC，如图 2-56 所示。

```
nltest /DCLIST:XXX
```

```
c:\Windows\Temp>nltest /DCLIST:hacke
获得域“hacke”中 DC 的列表<从“\DC”中>。
    DC.hacke.testlab [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成
```

图 2-56 查看域内控制器的机器名

2. 查看域控制器的主机名

执行如下命令，可以看到域控制器主机名为 dc，如图 2-57 所示。

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

```
c:\Windows\Temp>Nslookup -type=SRV _ldap._tcp
DNS request timed out.
    timeout was 2 seconds.
服务器:  Unknown
Address:  192.168.1.1

    _ldap._tcp.hacke.testlab      SRV service location:
        priority                = 0
        weight                   = 100
        port                     = 389
        srv_hostname              = dc.hacke.testlab
dc.hacke.testlab                internet address = 192.168.1.1
```

图 2-57 查看域控制器的主机名

3. 查看当前时间

一般时间服务器为主域控制器。执行如下命令，如图 2-58 所示。

```
net time /domain
```



```
c:\Windows\Temp>net time /domain
\\DC.hacke.testlab 的当前时间是 2018/12/2 22:05:35
命令成功完成。
```

图 2-58 查看当前时间

4. 查看域控制器组

执行如下命令，查看域控制器组。有一台域控制器的机器名为 DC，如图 2-59 所示。

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

```
c:\Windows\Temp>net group "Domain Controllers" /domain
这项请求将在域 hacke.testlab 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。
```

图 2-59 查看域控制器（1）

在真实环境中，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使域内服务验证正常进行。

执行如下命令，可以看到域控制器的机器名为 DC，如图 2-60 所示。

```
netdom query pdc
```

```
c:\Windows\Temp>netdom query pdc
域的主域控制器:
DC
命令成功完成。
```

图 2-60 查看域控制器（2）

2.9 获取域内的用户和管理员信息

2.9.1 查询所有域用户列表

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，如图 2-61 所示。域内存在四个用户，krbtgt 是用来创建票据授予服务（TGS）加密的密钥，它可以实现多种对域内持久化权限对方法，后面会一一讲解。

```
net user /domain
```



```
c:\Windows\Temp>net user /domain
这项请求将在域 hacke.testlab 的域控制器处理。

\DC.hacke.testlab 的用户帐户

-----
Administrator      Guest      krbtgt
testuser
命令成功完成。
```

图 2-61 向域控制器进行查询

2. 获取域内用户详细信息

执行如下命令，可以获取域内用户详细信息，常见参数包括用户名、描述信息、SID、域名、状态，如图 2-62 所示。

```
wmic useraccount get /all

Node,AccountType,Caption,Description,Disabled,Domain,FullName,InstallDate,LocalAccount,Lockout,Name>PasswordChangeable>PasswordExpires>PasswordR
WIN-HOC70E28R9B,512,WIN-HOC70E28R9B\Administrator,Built-in account for administering the computer/domain,FALSE,WIN-HOC70E28R9B,,,TRUE,FALSE,Admi
WIN-HOC70E28R9B,512,WIN-HOC70E28R9B\Guest,Guest,Built-in account for guest access to the computer/domain,TRUE,WIN-HOC70E28R9B,,,TRUE,FALSE,Guest,FALSE
WIN-HOC70E28R9B,512,PENTEST\Administrator,Built-in account for administering the computer/domain,FALSE,PENTEST,,,FALSE,FALSE,Administrator,TRUE,
WIN-HOC70E28R9B,512,PENTEST\Guest,Built-in account for guest access to the computer/domain,TRUE,PENTEST,,,FALSE,FALSE,Guest,FALSE,FALSE,S-
WIN-HOC70E28R9B,512,PENTEST\krbtgt,Key Distribution Center Service Account,TRUE,PENTEST,,,FALSE,FALSE,krbtgt,TRUE,TRUE,S-1-5-21-3112629480-
WIN-HOC70E28R9B,512,PENTEST\user1,,FALSE,PENTEST,,,FALSE,FALSE,user1,TRUE,TRUE,TRUE,S-1-5-21-3112629480-1751665795-4053538595-1104,1,OK
WIN-HOC70E28R9B,512,PENTEST\user1,,FALSE,PENTEST,qqq qq,,FALSE,FALSE,user1,TRUE,TRUE,TRUE,S-1-5-21-3112629480-1751665795-4053538595-1104,1,OK
```

图 2-62 获取域内用户详细信息

3. 查看存在的用户

执行如下命令，可以看到存在四个用户，如图 2-63 所示。

```
dsquery user

C:\Users\Administrator\Desktop>dsquery user
"CN=Administrator,CN=Users,DC=hacke,DC=testlab"
"CN=Guest,CN=Users,DC=hacke,DC=testlab"
"CN=krbtgt,CN=Users,DC=hacke,DC=testlab"
"CN=test,CN=Users,DC=hacke,DC=testlab"
```

图 2-63 查看存在的用户

常用的 dsquery 命令，如图 2-64 所示。

- 1 dsquery computer - 查找目录中的计算机。
- 2 dsquery contact - 查找目录中的联系人。
- 3 dsquery subnet - 查找目录中的子网。
- 4 dsquery group - 查找目录中的组。
- 5 dsquery ou - 查找目录中的组织单位。
- 6 dsquery site - 查找目录中的站点。
- 7 dsquery server - 查找目录中的 AD DC/LDS 实例。
- 8 dsquery user - 查找目录中的用户。
- 9 dsquery quota - 查找目录中的配额规定。
- 10 dsquery partition - 查找目录中的分区。
- 11 dsquery * - 用通用的 LDAP 查询来查找目录中的任何对象。

图 2-64 常用的 dsquery 命令



4. 查询域内置本地管理员组用户

执行如下命令，可以看到，本地管理员有两个用户和一个组，如图 2-65 所示。

```
net localgroup administrators /domain
```

```
C:\Users\user1>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
Administrator
Dm
PENTEST\Domain Admins
The command completed successfully.
```

图 2-65 查询域内置本地管理员组用户

默认 Domain Admins 组为域内机器的本地管理员用户。在真实环境中，为了方便管理，会有域用户被添加为域机器的本地管理员用户。

2.9.2 查询域管理员用户组

1. 查询域管理员用户

执行如下命令，可以看到存在两个域管理员用户，如图 2-66 所示。

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

```
C:\Users\user1>net group "domain admins" /domain
The request will be processed at a domain controller for domain pentest.com.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-----
Administrator      Dm
The command completed successfully.
```

图 2-66 查询域管理员用户

2. 查询管理员用户组

执行如下命令，看到管理员用户为 Administrator，如图 2-67 所示。

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



```

C:\Users\user1>net group "Enterprise Admins" /domain
The request will be processed at a domain controller for domain pentest.com.

Group name      Enterprise Admins
Comment         Designated administrators of the enterprise

Members

-----
Administrator
The command completed successfully.

```

图 2-67 查询管理员用户组

2.10 定位域管理员

2.10.1 域内定位管理员概述

内网渗透测试与常规的渗透测试是截然不同的。内网渗透测试的需求是拿到内网中特定用户或特定机器的权限，进而获得特定资源，完成内网渗透测试任务。在通常的网络环境里，内网中部署了大量的网络安全设备，如 IDS、IPS、日志审计、安全网关、反病毒软件等。所以，在域网络攻击测试场景中，如果渗透测试人员获取了域内的一个支点，为了实现对域网络的整体控制，渗透测试人员就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的权限。也就是说，在计算机添加到域中，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，域管理员组的成员均可访问本地计算机，而且具备完全控制权限。

渗透测试人员通常会通过搜集域内信息、追踪域内特权用户、域管理组用户的历史登录位置、当前登录位置等。定位域内管理员的常规渠道，一是日志，二是会话。日志是指本地机器的管理员日志，可以使用脚本或 `wevtutil` 导出查看。会话是指域内每个机器的登录会话，可以匿名查询，无须权限，可以使用 `netsess.exe` 或 `PowerView` 等工具查询。

2.10.2 常用域管理员定位工具

假设已经在 Windows 域中取得了普通用户权限，希望在域内横向移动，想知道域内用户登录的位置、他是否是任何系统中的本地管理员、他所归属的组、他是否有权访问文件共享等。枚举主机、用户和组，有助于我们更好地了解域内布局。

常用的工具有 `psloggedon.exe`、`pveFindADUser.exe`、`netsess.exe`、`hunter`、`NetView` 等。在 PowerShell 中，常用的脚本是 `PowerView`。

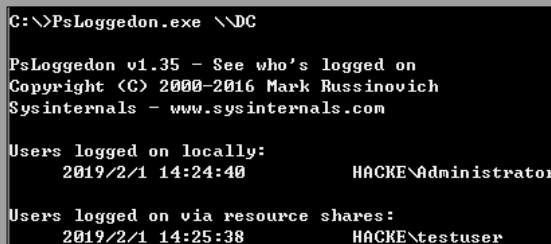
1. psloggedon.exe

在 Windows 中，可以使用命令“`net session`”查看谁在本地计算机上使用了资源，但是没有命令用来查看谁在使用远程计算机的资源、谁登录了本地或远程计算机。`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, 其原理是通过检验注册表里 HKEY_USERS 项的 key 值来查询谁登录过机器 (同样调用了 NetSessionEnum API), 某些功能需要拥有管理员权限才能使用。psloggedon.exe 的下载地址为 <https://docs.microsoft.com/en-us/sysinternals/downloads/psloggedon>, 使用如下命令及参数, 如图 2-68 所示。

```
psloggedon [-l] [-x] [\\computername|username]
```



```
C:\>PsLoggedon.exe \\DC

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

Users logged on locally:
2019/2/1 14:24:40      HACKE\Administrator

Users logged on via resource shares:
2019/2/1 14:25:38      HACKE\testuser
```

图 2-68 psloggedon.exe

- -: 显示支持的选项和用于输出值的单位。
- -l: 仅显示本地登录, 不显示本地和网络资源登录。
- -x: 不显示登录时间。
- \\computername: 指定要列出登录信息的计算机的名称。
- Username: 指定用户名, 在网络中搜索该用户登录的计算机。

2. pveFindADUser.exe

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 .NET Framework 2.0, 并且需要具有管理员权限。pveFindADUser.exe 的下载地址为 <https://github.com/chrisdee/Tools/tree/master/AD/ADFindUsersLoggedOn>, 使用如下命令及参数, 如图 2-69 所示。

```
pveFindADUser.exe <参数>
```

- -h: 显示帮助。
- -u: 检查是否有更新版本的实用程序。
- -current ["username"]: 如果仅指定了 -current 参数, 将获取所有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"]: 如果仅指定了 -last 参数, 将获取目标计算机上的最后一个登录用户。如果指定了用户名 (DOMAIN\Username), 则显示具有此用户账户作为上次登录的计算机。



根据网络的策略，可能会隐藏最后一个登录用户名，且该工具可能无法得到该用户名。

- -noping: 阻止该工具在尝试获取用户登录信息之前对目标计算机执行 ping 命令。
- -target: 可选参数，用于指定要查询的主机。如果未指定此参数，将查询当前域中的所有主机。如果指定此参数，则后跟一个由逗号分隔的主机名列表。

```
C:\>PUEFindADUser.exe -current

-----
PUE 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.hacke.testlab <Windows Server 2012 R2 Datacenter>
      - Logged on user : hacke\administrator
  [+] Processing host : WIN7-X64-TEST.hacke.testlab <Windows 7 旗舰版;Service Pack 1>
  [+] Processing host : WIN-2008.hacke.testlab <Windows Server 2008 R2 Datacenter>
[+] Report written to report.csv
```

图 2-69 pveFindADUser.exe

在最简单的形式中，直接运行“pveadfinduser.exe -current”命令，即可显示域中的所有计算机（计算机、服务器、域控制器等）上当前登录的所有用户。查询的结果会输出到一个文件 report.csv 中。

3. netview.exe

netview.exe 是一个枚举工具，使用 WinAPI 枚举系统，利用 NetSessionEnum 找寻登录会话，利用 NetShareEnum 找寻共享，利用 NetWkstaUserEnum 枚举登录的用户。同时，netview.exe 能够查询共享入口和有价值用户。netview.exe 的绝大部分功能不需要管理员权限即可执行，下载地址为 <https://github.com/mubix/netview>，使用如下命令及参数，如图 2-70 所示。

netview.exe <参数>

```
Enumerating AD Info
[+] WINDOWS2 - Comment -
[+] W - OS Version - 6.1

Enumerating IP Info
[+] <null> - IPv6 Address - fe80::7500:cecb:d078:8688%11
[+] <null> - IPv4 Address - 192.168.52.205

Enumerating Share Info
[+] WINDOWS2 - Share : ADMIN$ : Remote Admin
[+] Read access to: \\WINDOWS2\\ADMIN$
[+] WINDOWS2 - Share : C$ : Default share
[+] Read access to: \\WINDOWS2\\C$
[+] WINDOWS2 - Share : IPC$ : Remote IPC

Enumerating Session Info
[+] WINDOWS2 - Session - jasonf from \\[fe80::7500:cecb:d078:8688]
Idle: 0
```

图 2-70 netview.exe



- -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。

4. Nmap 的 NSE 脚本

如果有域账户或者本地账户, 就可以使用 Nmap 的 smb-enum-sessions.nse 引擎来获取远程机器的登录会话, 并且不需要管理员权限, 如图 2-71 所示。smb-enum-sessions.nse 的下载地址为 <https://nmap.org/nsedoc/scripts/smb-enum-sessions.html>。

```
Host script results:
| smb-enum-sessions:
|   Users logged in
|   TESTLAB\Administrator since <unknown>
|   Active SMB sessions
|   JASONF is connected from \\192.168.52.242
|_ ly you], idle for [not idle].
```

图 2-71 Nmap 的 NSE 脚本

- smb-enum-domains.nse: 对域控制器进行信息收集, 可以获取主机信息、用户、密码策略可以使用的用户等。
- smb-enum-users.nse: 在进行域渗透测试的时候, 如果获取了域内某台主机的权限, 但是权限有限, 不能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.nse: 遍历远程主机的共享目录。
- smb-enum-processes.nse: 对主机的系统进程进行遍历。通过这些信息, 可以知道目标主机上运行软件信息, 选择合适的漏洞或者规避防火墙及杀毒软件。
- smb-enum-sessions.nse: 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.nse: 收集目标主机的操作系统、计算机名、域名、全称域名、域名名称、NetBIOS 机器名、NetBIOS 域名、工作组、系统时间。

5. PowerView 脚本

PowerView 是一款 PowerShell 脚本, 里面有一些功能可以辅助找寻定位关键用户, 下载地址为 <https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView>。

- Invoke-StealthUserHunter: 只需要一次查询, 就可以获取域内的所有用户。从 user.HomeDirectories 中提取所有用户, 并对每个服务器进行 Get-NetSessions 获取。因为不需要使用 Invoke-UserHunter 对每台机器进行操作, 所以这个方法的隐蔽性相对较高, 但涉



及的机器面不一定完整。默认使用 Invoke-StealthUserHunter，如果找不到需要的信息，就接着使用 Invoke-UserHunter 方法。

- **Invoke-UserHunter**：找到域内特定的用户群。它接收用户名、用户列表或域组查询，并接收一个主机列表或查询可用的主机域名。它会使用 Get-NetSessions 和 Get-NetLoggedon（调用 NetSessionEnum 和 NetWkstaUserEnum API）扫描每个服务器，而且会比较结果，筛选出目标用户集。使用这个工具是不需要管理员权限的。在本地绕过执行该脚本，如图 2-72 所示。

```
C:\>powershell.exe -exec bypass -Command "& {Import-Module C:\PowerView.ps1; Invoke-UserHunter}"

UserDomain      : HACKE
UserName         : Administrator
ComputerName     : DC.hacke.testlab
IPAddress        : 1.1.1.2
SessionFrom      :
SessionFromName  :
LocalAdmin       :

UserDomain      : HACKE
UserName         : Administrator
ComputerName     : WIN-2008.hacke.testlab
IPAddress        : 1.1.1.10
SessionFrom      :
SessionFromName  :
LocalAdmin       :
```

图 2-72 Invoke-UserHunter

6. Empire 下的 user_hunter 模块

在 Empire 下也存在类似 Invoke-UserHunter 的模块——user_hunter，这个模块就是用来查找域管理员登录的机器的。

使用 usemodule situational_awareness/network/powerview/user_hunter 模块可以清楚地看到哪个用户登录了哪台主机。在这里，显示域管理员曾经登录了机器名为 WIN7-64.shuteer.testlab、IP 地址为 192.168.31.251 的机器，如图 2-73 所示。

```
(Empire: situational_awareness/network/powerview/user_hunter) > execute
(Empire: situational_awareness/network/powerview/user_hunter) >
Job started: Debug32_nm2w3

UserDomain      : SHUTEER
UserName         : Administrator
ComputerName     : WIN7-64.shuteer.testlab
IPAddress        : 192.168.31.251
SessionFrom      :
LocalAdmin       :

Invoke-UserHunter completed!
```

图 2-73 显示域管理员曾经登录过的机器



2.11 查找域管理进程

一个典型的域权限提升过程通常围绕着收集明文凭据或者通过 Mimikatz 来获得提升的权限等方法,然后在其所获取管理员权限的系统中寻找域管理员登录进程,从而收集域管理员的凭据。

如果在一个非常复杂的内网环境中,渗透测试人员不能立即在拥有权限的系统上获得域管理员进程,通常采用的方法是在跳板机之间进行跳转,直至获取域管理员权限,并进行一些分析工作,以找到其渗透测试路径。

我们来看一种假设的情况:渗透测试人员在某个内网环境中获得了一个域普通用户的权限,首先通过各种方法获得当前服务器的本地管理员权限,然后分析当前服务器的用户登录列表及会话信息,找出有哪些用户登录了这台服务器上。如果渗透测试人员通过分析发现,可以获取权限的登录用户都不是域管理员账户,同时也没有域管理员组的用户登录这台服务器,那么他会选择另一个账户,继续寻找这个账户在内网哪个机器上具有管理权限,再枚举这台机器上的登录用户,并继续进行渗透测试,直至找到一个有效的路径可以获取到域管理员权限为止。在具有成千上万台计算机和用户的环境中,该过程可能需要几天甚至几周的时间。

2.11.1 本机检查

1. 获取域管理员列表

执行如下命令,可以看到当前域管理员有两个,如图 2-74 所示。

```
net group "Domain Admins" /domain
```

```
PS C:\> net group "Domain Admins" /domain
这项请求将在域 hacke.testlab 的域控制器处理。

组名      Domain Admins
注释      指定的域管理员
成员

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

图 2-74 获取域管理员列表

2. 列出本机所有进程及进程用户

指定如下命令,列出本机所有进程及进程用户,如图 2-75 所示。

```
Tasklist /v
```

3. 寻找是否有进程所有者为域管理员的进程

当前存在域管理进程。通过对本机检查的方法,如果能够顺便找到域管理员进程是最好的,但有时实际情况并非这样。



GoogleCrashHandler.exe	756 Services	0	1,152 K Unknown	暂缺
GoogleCrashHandler64.exe	3088 Services	0	1,044 K Unknown	暂缺
csrss.exe	1380 Console	1	16,468 K Running	暂缺
winlogon.exe	3908 Console	1	6,796 K Unknown	暂缺
taskhost.exe	2040 Console	1	7,352 K Running	HACKER\testuser

图 2-75 查看进程

2.11.2 查询域控制器的域用户会话

查询域控制器的域用户会话，其原理是：在域控制器中查询域用户会话列表，并将其与域管理员列表交叉引用，从而找出域管理会话的系统列表。在这里，必须查询所有域控制器。

1. 查询域控制器列表

使用 LDAP 查询从 Domain Controllers 单元收集的域控制器的列表。也可以使用 net 命令查询域控制器列表，如下所示。

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

2. 收集域管理员列表

使用 LDAP 进行查询。也可以使用 net 命令从域管理员组中收集域管理员列表，如下所示。

```
net group "Domain Admins" /domain
```

3. 收集所有活动域会话列表

使用 Netsess.exe 查询每个域控制器，收集所有活动域会话列表。Netsess 是一个很棒的工具，它包含了本地 Windows 函数 netsessionenum，命令如下，如图 2-76 所示。该函数可以返回活动会话的 IP 地址、域账户、会话开始时间和空闲时间。

```
Netsess.exe -h
```



图 2-76 使用 Netsess.exe 收集所有活动域会话列表



4. 交叉引用域管理员列表与活动会话列表

将域管理员列表与活动会话列表进行交叉引用，以确定哪些 IP 地址具有活动域令牌。

在一个安全的环境中，可能需要等待具有域管理员权限的域管理员活动才能执行操作。所以，需要多次运行该过程，也可以使用下列脚本，快速使用 Netsess.exe 的 Windows 命令行。

将域控制器列表添加到 dcs.txt 中，将域管理员列表添加到 admins.txt 中，并和 netsess.exe 放在同一个目录下。运行如下脚本后，会在当前目录下生成一个 sessions.txt 文本文件，如图 2-77 所示。

```
FOR /F %i in (dcs.txt) do @echo [+] Querying DC %i && @netsess -h %i 2>nul >
sessions.txt && FOR /F %a in (admins.txt) DO @type sessions.txt | @findstr
/I %a
```

```
C:\>type sessions.txt
Enumerating Host: 1.1.1.2
Client          User Name          Time          Idle Time
-----
\\1.1.1.10      Administrator      000:00:00     000:00:00
Total of 1 entries enumerated
```

图 2-77 运行结果

网上也有类似的脚本，如 Get Domain Admins (GDA) 批处理脚本，它可以自动完成整个过程，下载地址为 <https://github.com/nullbind/Other-Projects/tree/master/GDA>。

2.11.3 扫描远程系统上运行的任务

如果渗透目标在域系统上使用共享本地管理员账户运行后，可以用下列脚本来扫描系统中的域管理任务。

同样首先从“域管理员”组中收集域管理员的列表。

```
net group "Domain Admins" /domain
```

然后使用下列脚本，其中 ips.txt 填入目标域系统的列表，在 names.txt 填入收集来的域管理员的列表。运行结果如图 2-78 所示。

```
FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P
password 2>NUL > output.txt && FOR /F %n in (names.txt) DO @type output.txt |
findstr %n > NUL && echo [!] %n was found running a process on %i && pause
```

```
C:\>FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P pass
word 2>NUL > output.txt && FOR /F %n in (names.txt) DO @type output.txt | findst
r %n > NUL && echo [!] %n was found running a process on %i && pause
[+] 1.1.1.2
```

图 2-78 运行结果



2.11.4 扫描远程系统上 NetBIOS 信息

在一些 Windows 系统中，允许用户通过 NetBIOS 查询已登录用户。下面这个 Windows 命令行脚本将扫描远程系统活跃域管理会话。

同样，先收集域管理员列表，然后将目标域系统列表添加到 ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，并置于同一目录下，如图 2-79 所示。

```
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtstat -A %i 2>NUL >nbse  
ssions.txt && FOR /F %n in (admins.txt) DO @type nbse  
ssions.txt ! findstr /I %n  
> NUL && echo [!] %n was found logged into %i
```

```
C:\>for /F %i in (ips.txt) do @echo [+] Checking %i && nbtstat -A %i 2>NUL >nbse  
ssions.txt && FOR /F %n in (admins.txt) DO @type nbse  
ssions.txt ! findstr /I %n  
> NUL && echo [!] %n was found logged into %i  
[+] Checking 1.1.1.2
```

图 2-79 运行结果 (1)

同样，在这里也可以使用 nbtscan 工具。先收集域管理员列表，然后将目标域系统列表添加到 ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，和 nbtscan 工具置于同一目录下，如图 2-80 所示。

```
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i  
2>NUL >nbse  
ssions.txt && FOR /F %n in (admins.txt) DO @type nbse  
ssions.txt ! findstr /I %n  
> NUL && echo [!] %n was found logged into %i
```

```
C:\>for /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i 2>NUL >nbse  
ssions.txt && FOR /F %n in (admins.txt) DO @type nbse  
ssions.txt ! findstr /I %n  
> NUL && echo [!] %n was found logged into %i  
[+] Checking 1.1.1.2
```

图 2-80 运行结果 (2)

2.12 模拟域管理员方法简介

如果您已经有一个 meterpreter 会话，您可以使用 Incognito 模拟域管理员，或添加一个新的域管理员。通过尝试遍历系统中所有可用的授权令牌来随意添加新的管理员。具体操作方法在第四章中会详细讲解。

2.13 利用 PowerShell 收集域信息

PowerShell 是微软推出的一款用于提高管理员对操作系统及应用程序易用性和扩展性的脚本环境，可以说是 cmd.exe 的加强版。微软已经将 PowerShell 2.0 内置在 Windows Server 2008 和 Windows 7 中，将 PowerShell 3.0 内置在 Windows Server 2012 和 Windows 8 中，将 PowerShell 4.0



内置在 Windows Server 2012 R2 和 Windows 8.1 中，将 PowerShell 5.0 内置在 Windows Server 2016 和 Windows 10 中。PowerShell 作为微软官方推出的脚本语言，在 Windows 系统中的强大众所周知：在系统管理员手中，可以提高 Windows 系统管理工作的自动化程度；在渗透测试人员手中，便于渗透测试人员更好地绕过系统防护和相关反病毒软件。

如果想在 Windows 系统中执行一个 PowerShell 脚本，首先需要在 Windows 系统的“开始菜单”中打开“Run”对话框，输入“powershell”，如图 2-81 所示。

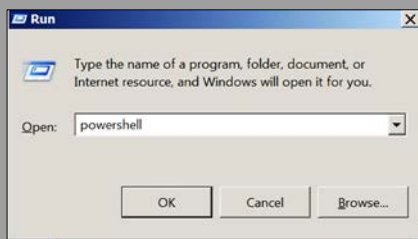


图 2-81 输入“powershell”

接下来，将弹出一个窗口，窗口上方有“Administrator”字样，代表当前 PowerShell 权限为管理员权限，如图 2-82 所示。

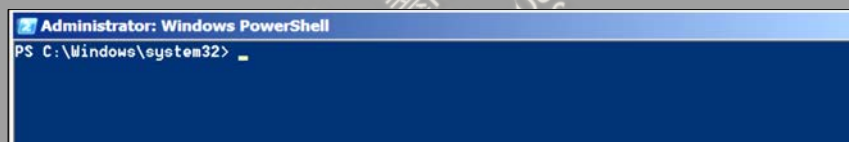


图 2-82 PowerShell 弹窗

如果想执行一个 PowerShell 脚本，需要修改 PowerShell 的默认权限为执行权限。PowerShell 常用的执行权限共有四种，具体如下。

- Restricted：默认设置，不允许执行任何脚本。
- Allsigned：只能运行经过证书验证的脚本。
- Unrestricted：权限最高，可以执行任意脚本。
- RemoteSigned：本地脚本无限制，但是对来自网络的脚本必须经过签名。

在 PowerShell 中输入“Get-ExecutionPolicy”，看到为默认 Restricted 权限，如图 2-83 所示。

```
PS C:\Windows\system32> Get-ExecutionPolicy
Restricted
PS C:\Windows\system32>
```

图 2-83 查看当前 PowerShell 执行权限

将 PowerShell 执行权限改为 Unrestricted，输入“Y”，如图 2-84 所示。



```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic. Do you want to change the execution
policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Windows\system32>
```

图 2-84 修改 PowerShell 执行权限

PowerView 是一款依赖 PowerShell 和 WMI 对内网域情况进行查询的常用渗透脚本。

PowerView 集成在 PowerSploit 工具包中，下载地址为 <https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1>。

打开一个 PowerShell 窗口，进入 PowerSploit 目录下的 Recon 目录，输入命令 “Import-Module .\PowerView.ps1”，成功导入脚本，没有报错，如图 2-85 所示。

```
PS C:\Windows\system32> cd C:\Users\user1\Desktop\PowerSploit-master\Recon
PS C:\Users\user1\Desktop\PowerSploit-master\Recon> Import-Module .\PowerView.ps1
PS C:\Users\user1\Desktop\PowerSploit-master\Recon>
```

图 2-85 导入 PowerView.ps1 脚本

PowerView 中的常用命令如下。

- Get-NetDomain：获取当前用户所在的域名称。
- Get-NetUser：返回所有用户的详细信息。
- Get-NetDomainController：获取所有域控制器。
- Get-NetComputer：获取所有域内机器的详细信息。
- Get-NetOU：获取域中的 OU 信息。
- Get-NetGroup：获取所有域内组和组成员信息。
- Get-NetFileServer：根据 SPN 获取当前域使用的文件服务器。
- Get-NetShare：获取当前域内所有网络共享。
- Get-NetSession：获取在指定服务器存在的会话信息。
- Get-NetRDPSession：获取在指定服务器存在的远程连接信息。
- Get-NetProcess：获取远程主机的进程信息。
- Get-UserEvent：获取指定用户的日志信息。
- Get-ADObject：获取活动目录的对象信息。
- Get-NetGPO：获取域所有组策略对象。
- Get-DomainPolicy：获取域默认或域控制器策略。
- Invoke-UserHunter：用于获取域用户登录计算机及该用户是否有本地管理权限。
- Invoke-ProcessHunter：查找域内所有机器进程用于找到某特定用户。
- Invoke-UserEventHunter：根据用户日志获取某域用户登录过哪些域机器。

