内网信息收集

AUTOR@伊恒

概述:

在我们进行内网渗透时，我们会先对当前网络环境进行观察判断，洞察内网中的拓扑图结构，找出内网中薄弱的环节。判断是我们一般都是涉及以下三个方面。
我是谁 对当前机器角色的判断(指判断当前机器是web服务器，文件服务器，还是DNS服务器)
这是哪 对当前所处网络环境的拓扑图结构进行分析和判断(对当前网络环境绘制出大致拓扑图)
我在哪 对当前机器所在内网环境进行判断(判断当前机器是DMZ还是办公区)

收集本机信息:

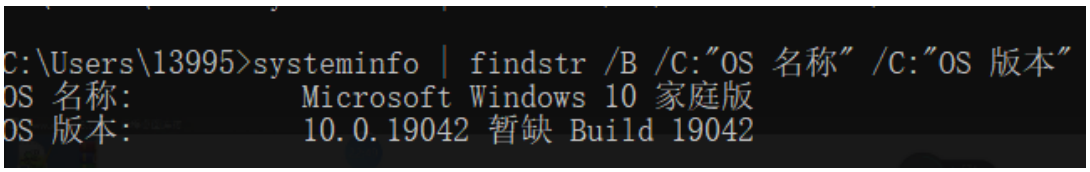
1.查询网络配置信息

```
ipconfig/all
```

2.查询操作系统和软件信息

(1)查询操作系统和版本信息

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
```



(2)查看系统体系结构

```
echo %PROCESSOR_ARCHITECTURE%
```

(3)查看安装的软件即版本，路径等

利用wmic命令

```
wmic product get name,version
```

```
C:\Users\13995>wmic product get name,version
Name                                                  Version
Python 3.9.6 Executables (32-bit)                     3.9.6150.0
Python 3.9.6 Utility Scripts (32-bit)                 3.9.6150.0
Python 3.9.6 pip Bootstrap (32-bit)                   3.9.6150.0
Python 3.9.6 Test Suite (32-bit)                      3.9.6150.0
Python 3.9.6 Documentation (32-bit)                   3.9.6150.0
Python 3.9.6 Add to Path (32-bit)                     3.9.6150.0
Python 3.9.6 Core Interpreter (32-bit)                3.9.6150.0
Python 3.9.6 Standard Library (32-bit)                3.9.6150.0
Python 3.9.6 Development Libraries (32-bit)           3.9.6150.0
Python 3.9.6 Tcl/Tk Support (32-bit)                  3.9.6150.0
Office 16 Click-to-Run Extensibility Component        16.0.14701.20226
Office 16 Click-to-Run Localization Component         16.0.14701.20210
```

利用powershell

```
powershell "Get-WmiObject -class Win32_Product | Select-Object -Property name, version"
```

```
C:\Users\13995>powershell "Get-WmiObject -class Win32_Product | Select-Object -Property name, version"

name                                  version
----                                  -------
Python 3.9.6 Executables (32-bit)     3.9.6150.0
Python 3.9.6 Utility Scripts (32-bit) 3.9.6150.0
```

3.查询本机服务信息

```
wmic service list brief
```

```
C:\Users\13995>wmic service list brief
ExitCode  Name                        ProcessId  StartMode  State    Status
1077      AJRouter                    0          Manual     Stopped  OK
0         ALG                         0          Manual     Stopped  OK
1077      AntiCheatExpert Service     0          Manual     Stopped  OK
1077      AppIDSvc                    0          Manual     Stopped  OK
0         Appinfo                     11064      Manual     Running  OK
1077      AppReadiness                0          Manual     Stopped  OK
0         AppXSvc                     5580       Manual     Running  OK
0         AudioEndpointBuilder        3792       Auto       Running  OK
```

4.查询进程列表

```
tasklist  查看进程列表和用户
wmic process list brief  查看进程信息
```

```
C:\Users\13995>tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        132 K
Registry                       124 Services                   0     82,468 K
```

```
C:\Users\13995>wmic process list brief
HandleCount  Name                        Priority  ProcessId  ThreadCount  WorkingSetSize
0            System Idle Process        0         0          8            8192
7170         System                     8         4          228          135168
0            Registry                   8         124        4            84443136
```

5.查看启动项

```
wmic startup get command,caption
```

```
C:\Users\13995>wmic startup get command,caption
Caption                  Command
OneDrive                 "C:\Program Files (x86)\Microsoft OneDrive\OneDriv
Wechat                   D:\微信\WeChat\WeChat.exe
CCleaner Smart Cleaning  "D:\cclearn\CCleaner64.exe" /MONITOR
BaiduYunGuanjia          "D:\baidu网盘\BaiduNetdisk\baidunetdisk.exe" AutoR
BaiduYunDetect           "D:\baidu网盘\BaiduNetdisk\YunDetectService.exe"
Steam                    "D:\steam\steam.exe" -silent
Dingtalk                 D:\钉钉\DingDing\DingtalkLauncher.exe /autorun
```

6.查看计划任务

```
schtasks /query /fo LIST /v
```

```
C:\Users\13995>schtasks /query /fo LIST /v

文件夹: \
主机名:                                DESKTOP-PH7U90V
任务名:                                \360wp-srv
下次运行时间:                          N/A
模式:                                  正在运行
登录状态:                              只使用交互方式
上次运行时间:                          2021/12/16 17:20:04
上次结果:                              267009
创建者:                                13995
要运行的任务:                          "C:\Program Files (x86)\BirdWallpap
起始于:                                N/A
注释:                                  Starts 360wp-srv when a user logs o
计划任务状态:                          已启用
空闲时间:                              已禁用
电源管理:
作为用户运行:                          13995
删除没有计划的任务:                    已禁用
如果运行了 X 小时 X 分钟，停止任务:    已禁用
计划:                                  计划数据在此格式中不可用。
计划类型:                              登陆时
开始时间:                              N/A
开始日期:                              N/A
结束日期:                              N/A
天:                                    N/A
月:                                    N/A
```

7.查看开机时间

```
net statistics workstation
```

```
C:\Users\13995>net statistics workstation
\\DESKTOP-PH7U90V 的工作站统计数据

统计数据开始于 2021/12/15 12:48:53

接收的字节数                    184052
接收的服务器消息块 (SMB)        78
传输的字节数                    165406
传输的服务器消息块 (SMB)        0
读取操作                        0
写入操作                        0
拒绝原始读取                    0
拒绝原始写入                    0

网络错误                        0
已做连接                        0
重新连接                        0
服务器断开连接                  0
```

8.查询用户列表

查看本机用户列表

```
net user
```

```
C:\Users\13995>net user

\\DESKTOP-PH7U90V 的用户帐户

-------------------------------------------------------------------------------
13995                    Administrator            DefaultAcco
Guest                    test                     WDAGUtility
```

获取本地管理员

```
net localgroup administrators
```

```
C:\Users\13995>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

-------------------------------------------------------------------------------
13995
Administrator
命令成功完成。
```

9.列出或断开本地计算机与所连接的客户端之间的会话

```
net session
```

```
C:\WINDOWS\system32>net session
列表是空的。
```

10.查询断开列表

```
netstat -ano
```

```
C:\Users\13995>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       2772
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       17192
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1208
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING       6208
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       6492
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       6492
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       6592
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9120
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4392
  TCP    0.0.0.0:20531          0.0.0.0:0              LISTENING       6576
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       964
```

11.查看补丁列表

```
systeminfo
```

```
域:                        WORKGROUP
登录服务器:                \\DESKTOP-PH7U90V
修补程序:                  安装了 13 个修补程序。
                           [01]: KB5007289
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4577266
                           [05]: KB4577586
                           [06]: KB4580325
                           [07]: KB4586864
                           [08]: KB4589212
                           [09]: KB4593175
                           [10]: KB4598481
                           [11]: KB5007186
```

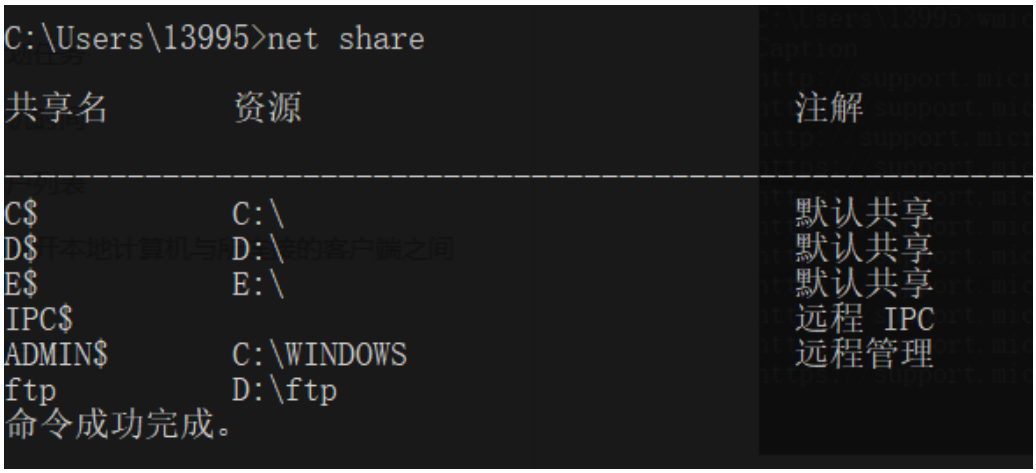
查看补丁具体信息

```
wmic qfe get Caption,Description,HotFixID,InstalledOn
```

```
C:\Users\13995>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                      Description      HotFixID   InstalledOn
http://support.microsoft.com/?kbid=5007289   Update           KB5007289  12/1/2021
https://support.microsoft.com/help/4562830   Update           KB4562830  12/12/2020
http://support.microsoft.com/?kbid=4570334   Security Update  KB4570334  9/27/2020
https://support.microsoft.com/help/4577266   Security Update  KB4577266  10/9/2020
https://support.microsoft.com/help/4577586   Update           KB4577586  3/10/2021
https://support.microsoft.com/help/4580325   Security Update  KB4580325  10/9/2020
https://support.microsoft.com/help/4586864   Security Update  KB4586864  11/29/2020
https://support.microsoft.com/help/4589212   Update           KB4589212  3/12/2021
https://support.microsoft.com/help/4593175   Security Update  KB4593175  12/12/2020
https://support.microsoft.com/help/4598481   Security Update  KB4598481  1/13/2021
https://support.microsoft.com/help/5007186   Security Update  KB5007186  11/12/2021
                                             Update           KB5006753  11/12/2021
                                             Security Update  KB5005699  9/17/2021
```

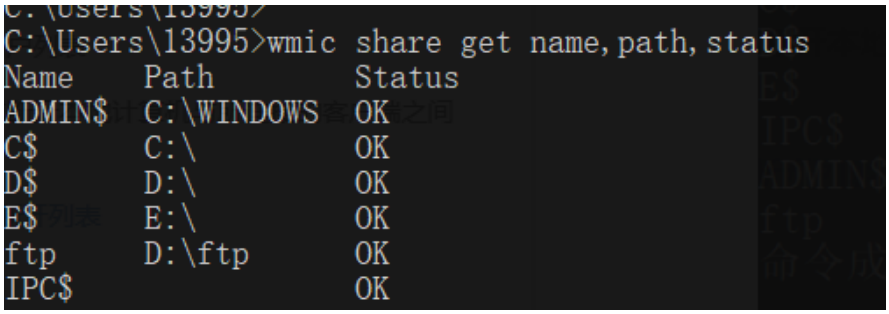
12.查看本机共享列表

```
net share
```



利用wmic命令查找共享列表

```
wmic share get name,path,status
```



13.查询路由表及所有可用接口的ARP

```
route print
arp -a
```

14.查看防火墙配置

(1)关闭防火墙

win server2k3及以前

```
netsh firewall set opmode disable
```

win server2k3之后的版本

```
netsh advfirewall set allprofiles state off
```

(2)查看防火墙配置

```
netsh firewall show config
```

(3)修改防火墙配置

win server2k3及以前

```
netsh firewall add allowedprogram c:\nc.exe "allow nc" enable
```

win server2k之后的版本
允许指定程序进入：

```
netsh advfirewall firewall add rule name="pass nc" dir=in action=allow pro
gram="C:\nc.exe"
```

允许指定程序退出：

```
netsh advfirewall firewall add rule name="pass nc" dir=out action=allow pr
ogram="C:\nc.exe"
```

允许3389端口放行：

```
netsh advfirewall firewall add rule name="Remote Desktop" protocol=TCP dir
=in localport=3389 action=allow
```

15.查询并开启远程连接服务

(1)查看远程连接端口

```
REG QUERY"HKEY_ LOCAL MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Se
rver\WinStations\RDP-Tcp" /V Por tNumber
```

(2)在wind server 2k3 中开启3389端口

```
wmic path win32_terminalservicesetting where (__CLASS !="") call setallowt
sconnections 1
```

(3)在wind server 2k8和wind server 2012中开启3389端口

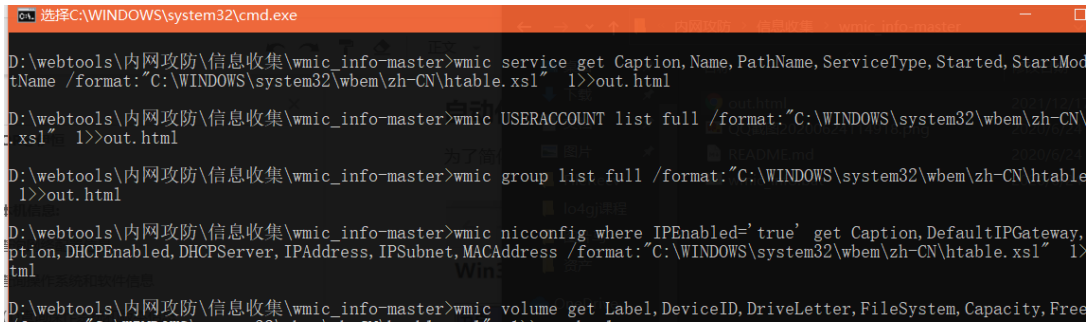
```
wmic /namespace:\\root\cimv2\terminalservices path win32_terminalservicese
tting  where (__CLASS !="") call setallowtsconnections 1
```

```
wmic /namespace:\\root\cimv2\terminalservices path win32_tsgeneralsetting
 where (TerminalName='RDP-Tcp') call setuserauthenticationrequired 1
```

```
reg add "HKLM\SYSTEM\CURRENT\CONTROLSET\CONTROL\TERMINAL SERVER" /v fSingl
eSessionPerUser /t REG_DWORD /d 0 /f
```

自动化信息收集

为了简化上面的操作，我们可以制定一个bat文件wmic_info下载链接：https://github.com/gysf666/wmic_info



Empire下的主机信息收集

Empire提供用于收集主机信息的模块。
查看本机用户，域组成员，密码设置时间，剪切板内容，系统基本信息，网路适配器，共享信息等。

```
usermodule situational_awareness/host/winenum
```