

# 渗透测试 | 内网信息收集

Allex 天德网络安全 2020-05-29 20:39:06

请点击上面  u3000 一键关注!

内容来源：先知社区



## 前言

在内网渗透测试中，信息收集的深度与广度，直接关系到整个内网渗透测试的成败，本篇文章主要对内网信息收集做简单介绍~

## 一、内网信息描述

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其主机名、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。

## 二、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。

### 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。

#### 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，如图所示：

```
ipconfig /all
```

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

## Windows IP 配置

```
主机名 . . . . . : win-server-test
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-29-24-C5-83
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
本地连接 IPv6 地址. . . . . : fe80::cc02:583f:61e9:8f14%11(首选)
IPv4 地址 . . . . . : 192.168.174.4(首选)
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . :
DHCPv6 IAID . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-25-44-7B-0E-00-0C-29-85-82-82

DNS 服务器 . . . . . : 192.168.174.2
TCP/IP 上的 NetBIOS . . . . . : 已启用
```

## 隧道适配器 isatap.{72713B24-668C-4F4C-A3BD-65671104587B}:

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

## 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. . . . . : Teredo Tunneling Pseudo-Interface
物理地址. . . . . : 00-00-00-00-00-00-00-E0
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
```

```
C:\Users\testuser>_
```

查询操作系统版本

获取操作系统和版本信息

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

```
C:\Users\testuser>systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
OS 名称:      Microsoft Windows Server 2008 R2 Enterprise
OS 版本:      6.1.7601 Service Pack 1 Build 7601
```

```
C:\Users\testuser>_
```

执行以上命令，可以看到当前系统为Windows Server 2008 R2 Enterprise。如果是英文操作系统，则输入如下命令：

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

查看系统体系结构

执行如下命令，查看系统体系结构，如下图所示：



天億网络安全

先知社区

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



安装软件版本信息

使用wmic命令，可以将结果输出到文本中，具体如下，如下图所示：

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

```
C:\Users\testuser>wmic product get name,version
```

Name	Version
UMware Tools	10.3.10.12406962
Microsoft Visual C++ 2017 x86 Additional Runtime - 14.12.25810	14.12.25810
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810	14.12.25810
Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.12.25810	14.12.25810
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810	14.12.25810

```
C:\Users\testuser>
```



也可以利用PowerShell命令，收集软件版本信息条具体如下，如下图所示：

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

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

name	version
UMware Tools	10.3.10.12406962
Microsoft Visual C++ 2017 x86 Additi...	14.12.25810
Microsoft Visual C++ 2017 x64 Additi...	14.12.25810
Microsoft Visual C++ 2017 x86 Minimu...	14.12.25810
Microsoft Visual C++ 2017 x64 Minimu...	14.12.25810

```
C:\Users\testuser>
```



查询本机服务信息

执行如下命令，查询本机服务信息，如下图所示：

```
wmic service listbrief
```

C:\Users\testuser>wmic service list brief

ExitCode	Name	ProcessId	StartMode	State	Status
0	AeLookupSvc	832	Manual	Running	OK
1077	ALG	0	Manual	Stopped	OK
1077	AppIDSvc	0	Manual	Stopped	OK
0	Appinfo	832	Manual	Running	OK
1077	AppMgmt	0	Manual	Stopped	OK
1077	AudioEndpointBuilder	0	Manual	Stopped	OK
1077	AudioSrv	0	Manual	Stopped	OK
0	BFE	380	Auto	Running	OK
1077	BITS	0	Manual	Stopped	OK
1077	Browser	0	Disabled	Stopped	OK
1077	CertPropSvc	0	Manual	Stopped	OK
1077	clr_optimization_v2.0.50727_32	0	Manual	Stopped	OK
1077	clr_optimization_v2.0.50727_64	0	Manual	Stopped	OK
0	COMSysApp	1572	Manual	Running	OK
0	CryptSvc	1000	Auto	Running	OK
0	DcomLaunch	604	Auto	Running	OK
1077	defragsvc	0	Manual	Stopped	OK
0	Dhcp	772	Auto	Running	OK
0	Dnscache	1000	Auto	Running	OK
1077	dot3svc	0	Manual	Stopped	OK
0	DPS	380	Auto	Running	OK
1077	EapHost	0	Manual	Stopped	OK
1077	EFS	0	Manual	Stopped	OK
0	eventlog	772	Auto	Running	OK
0	EventSystem	884	Auto	Running	OK
1077	FCRegSvc	0	Manual	Stopped	OK
1077	fdPHost	0	Manual	Stopped	OK
1077	FDResPub	0	Manual	Stopped	OK

查询进程列表信息

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，如下图所示：

tasklist/v

C:\Users\testuser>tasklist /v

映像名称	PID	会话名	会话#	内存使用	状态	用户名
	CPU	时间 窗口标题				
=====						
System Idle Process	0	Services	0	24 K	Unknown	NT AUTHORITY\SYSTEM
System	1:25:39	暂缺	0	368 K	Unknown	暂缺
smss.exe	4	Services	0	1,012 K	Unknown	暂缺
	0:00:13	暂缺				
csrss.exe	224	Services	0	5,244 K	Unknown	暂缺
	0:00:00	暂缺				
wininit.exe	316	Services	0	4,684 K	Unknown	暂缺
	0:00:00	暂缺				
services.exe	368	Services	0	12,316 K	Unknown	暂缺
	0:00:02	暂缺				
lsass.exe	472	Services	0	12,368 K	Unknown	暂缺
	0:00:01	暂缺				
lsass.exe	480	Services	0	4,128 K	Unknown	暂缺
	0:00:00	暂缺				
suchost.exe	488	Services	0	9,288 K	Unknown	暂缺
	0:00:01	暂缺				
vmacthlp.exe	604	Services	0	4,240 K	Unknown	暂缺
	0:00:00	暂缺				
suchost.exe	664	Services	0	7,800 K	Unknown	暂缺
	0:00:01	暂缺				
suchost.exe	696	Services	0	12,056 K	Unknown	暂缺
	0:00:01	暂缺				
suchost.exe	772	Services	0	34,284 K	Unknown	暂缺
	0:00:01	暂缺				
suchost.exe	832	Services	0			

执行如下命令也可以查看进程信息：

wmic process listbrief

C:\Users\testuser>wmic process list brief

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	1	24576
469	System	8	4	85	376832
29	smss.exe	11	224	2	1036288
403	csrss.exe	13	316	9	5369856
78	wininit.exe	13	368	3	4796416
224	services.exe	9	472	9	12627968
643	lsass.exe	9	480	8	12681216
146	lsm.exe	8	488	11	4235264
348	svchost.exe	8	604	11	9510912
53	vmacthlp.exe	8	664	3	4341760
246	svchost.exe	8	696	8	7987200
292	svchost.exe	8	772	13	12341248
915	svchost.exe	8	832	32	35512320
533	svchost.exe	8	884	11	11968512
190	svchost.exe	8	952	6	10129408
413	svchost.exe	8	1000	17	15978496
295	svchost.exe	8	380	17	11812864
263	spoolsv.exe	8	1028	12	11071488
44	svchost.exe	8	1112	3	2699264
86	UGAuthService.exe	8	1152	3	8740864
187	vmtoolsd.exe	13	1192	9	16834560
255	WmiPrvSE.exe	8	1524	10	14716928
189	dllhost.exe	8	1572	13	11673600
145	msdtc.exe	8	1668	12	8015872
182	csrss.exe	13	2280	9	5586944
96	winlogon.exe	13	2304	3	

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，如下表所示：

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
EGULEXE	NoD32
AVP.exe	卡巴斯基
AVGUARD.exe	小红伞
BDAGENT.exe	BITDEFENDER

查看启动程序信息  
执行如下命令查看启动程序信息，如下图所示：

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

```
C:\Users\testuser>wmic startup get command,caption
Caption Command
UMware User Process "C:\Program Files\UMware\UMware Tools\umtoolsd.exe" -n vmusr
```

```
C:\Users\testuser>
```

查看计划任务信息

执行如下命令，查看计划任务，如下图所示：

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

```
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 X 小时 X 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: 当事件发生时
开始时间: N/A
开始日期: N/A
结束日期: N/A
天: N/A
月: N/A
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\AUSessionCo
nnect
下次运行时间: N/A
模式: 已禁用
微软拼音 半 :寸
```

PS: 如果遇到资源无法加载问题，则是由于当前活动页码所致：

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

错误：无法加载列资源。

```
C:\Users\testuser>chcp
```

活动代码页：936

```
C:\Users\testuser>
```

之后，我们可以将活动页码修改为437即可：

```
chcp437
```



Active code page: 437

C:\Users\testuser>\_



之后再次执行即可查看到相关计划任务信息:

```

Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background
Last Run Time: N/A
Last Result: 1
Author: Microsoft Corporation
Task To Run: COM handler
Start In: N/A
Comment: ????????????????
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management:
Run As User: INTERACTIVE
Delete Task If Not Rescheduled: Enabled
Stop Task If Runs X Hours and X Mins: Disabled
Schedule: Scheduling data is not available in this format.
Schedule Type: On demand only
Start Time: N/A
Start Date: N/A
End Date: N/A
Days: N/A
Months: N/A
Repeat: Every: N/A
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A

```

```

Folder: \Microsoft\Windows\Tcpip
HostName: WIN-SERVER-TEST
TaskName: \Microsoft\Windows\Tcpip\IpAddressConflict1
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background
Last Run Time: N/A

```

查看主机开机时间

执行如下命令, 查看主机开机时间, 如下图所示:



[回到顶部](#)

```
C:\Users\testuser>net statistics workstation
\\WIN-SERVER-TEST 的工作站统计数据
```

统计数据开始于 2020/2/13 23:39:17

接收的字节数	4965
接收的服务器消息块 (SMB)	29
传输的字节数	789
传输的服务器消息块 (SMB)	7
读取操作	11
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	1
重新连接	0
服务器断开	0
启动的会话	0
会话挂起	0
失败的会话	0
失败的操作	0
使用计数	14
使用计数失败	0

命令成功完成。



```
C:\Users\testuser>
```

查询用户列表信息

执行如下命令，查看本机用户列表，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：

```
netuser
```

```
C:\Users\testuser>net user
\\WIN-SERVER-TEST 的用户帐户
```

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



```
C:\Users\testuser>
```

先知社区

执行如下命令，获取本地管理员（通常含有域用户）信息：

```
netlocalgroup administrators
```



```
C:\Users\testuser>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

```
-----
Administrator
HACKE\Domain Admins
命令成功完成。
```

```
C:\Users\testuser>
```



执行如下命令，查看当前在线用户信息

```
query user ||qwinsta
```

```
C:\Users\testuser>query user || qwinsta
```

用户名	会话名	ID	状态	空闲时间	登录时间
>testuser	console	2	运行中	无	2020/2/13 23:40
会话名	用户名	ID	状态	类型	设备
services		0	断开		
>console	testuser	2	运行中		



```
C:\Users\testuser>
```

查客户端会话信息

执行如下命令(需要管理员权限才行)，列出或断开本地计算机和连接的客户端的会话，如下图所示：

```
net session
```

 管理员：命令提示符

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

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

```
C:\Windows\system32>
```



查询端口列表信息

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
```

C:\Users\testuser>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	696	
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	368	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	772	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	832	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	472	
TCP	0.0.0.0:64771	0.0.0.0:0	LISTENING	480	
TCP	0.0.0.0:64815	0.0.0.0:0	LISTENING	2440	
TCP	192.168.174.4:139	0.0.0.0:0	LISTENING	4	
TCP	192.168.174.4:64861	192.168.174.2:135	ESTABLISHED	480	
TCP	192.168.174.4:64862	192.168.174.2:49158	ESTABLISHED	480	
TCP	192.168.174.4:64869	192.168.174.2:445	ESTABLISHED	4	
TCP	:::135	:::0	LISTENING	696	
TCP	:::445	:::0	LISTENING	4	
TCP	:::47001	:::0	LISTENING	4	
TCP	:::49152	:::0	LISTENING	368	
TCP	:::49153	:::0	LISTENING	772	
TCP	:::49154	:::0	LISTENING	832	
TCP	:::49155	:::0	LISTENING	472	
TCP	:::64771	:::0	LISTENING	480	
TCP	:::64815	:::0	LISTENING	2440	
UDP	0.0.0.0:123	*:*		884	
UDP	0.0.0.0:500	*:*		832	
UDP	0.0.0.0:4500	*:*		832	
UDP	0.0.0.0:5355	*:*		1000	
UDP	127.0.0.1:58401	*:*		480	
UDP	127.0.0.1:58404	*:*		832	
UDP	127.0.0.1:65531	*:*		1000	
UDP	192.168.174.4:137	*:*		4	
UDP	192.168.174.4:138	*:*		4	
UDP	:::123	*:*		884	



从上图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。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。

查询补丁列表信息  
执行如下命令，查看系统的详细信息，需要注意系统的版本、位数、域、补丁信息及更新频率等。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2个补，如下图所示

Systeminfo

C:\Users\testuser>Systeminfo

```

主机名: WIN-SERUER-TEST
OS 名称: Microsoft Windows Server 2008 R2 Enterprise
OS 版本: 6.1.7601 Service Pack 1 Build 7601
OS 制造商: Microsoft Corporation
OS 配置: 成员服务器
OS 构件类型: Multiprocessor Free
注册的所有人: Windows 用户
注册的组织:
产品 ID: 00486-OEM-8400691-20006
初始安装日期: 2019/10/25, 17:40:09
系统启动时间: 2020/2/13, 23:39:06
系统制造商: VMware, Inc.
系统型号: VMware Virtual Platform
系统类型: x64-based PC
处理器: 安装了 1 个处理器。
[01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~2592 Mhz
BIOS 版本: Phoenix Technologies LTD 6.00, 2018/4/13
Windows 目录: C:\Windows
系统目录: C:\Windows\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (UTC+08:00)北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 2,047 MB
可用的物理内存: 1,600 MB
虚拟内存: 最大值: 4,095 MB
虚拟内存: 可用: 3,653 MB
虚拟内存: 使用中: 442 MB
页面文件位置: C:\pagefile.sys
域: hacke.testlab
登录服务器: \\DC
修补程序: 安装了 2 个修补程序。
[01]: KB2999226
[02]: KB976902
网卡: 安装了 1 个 NIC。
[01]: Intel(R) PRO/1000 MT Network Connection
连接名: 本地连接
    
```



同时, 也可以使用wmic来识别安装在系统中的补丁情况, 命令如下图所示:

wmic qfe get Caption,Description,HotFixID,InstalledOn

```

C:\Users\testuser>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption Description HotFixID InstalledOn
http://support.microsoft.com/?kbid=2999226 Update KB2999226 10/25/2019
http://support.microsoft.com/?kbid=976902 Update KB976902 11/21/2010
    
```



C:\Users\testuser>\_

先知社区

从上面的执行结果, 我们可以看到补丁的名称、描述、补丁ID、安装时间等信息。

查看本机共享信息

执行如下命令, 可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), 如下图所示:

netshare

C:\Users\testuser>net share

共享名	资源	注解
C\$	C:\	默认共享
IPC\$		远程 IPC
ADMIN\$	C:\Windows	远程管理

命令成功完成。



C:\Users\testuser>\_

先知社区

利用wmic查找共享, 命令如下:

wmic share getname,path,status

```
C:\Users\testuser>wmic share get name,path,status
```

```
Name      Path      Status
ADMIN$    C:\Windows OK
C$        C:\       OK
IPC$      OK
```

```
C:\Users\testuser>
```



查询路由和缓存表

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：

```
route print
```

```
C:\Users\testuser>route print
```

接口列表

```
11...00 0c 29 24 c5 83 .....Intel(R) PRO/1000 MT Network Connection
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
```

IPv4 路由表

活动路由：

网络目标	网络掩码	网关	接口	跃点数
127.0.0.0	255.0.0.0		在链路上	127.0.0.1 306
127.0.0.1	255.255.255.255		在链路上	127.0.0.1 306
127.255.255.255	255.255.255.255		在链路上	127.0.0.1 306
192.168.174.0	255.255.255.0		在链路上	192.168.174.4 266
192.168.174.4	255.255.255.255		在链路上	192.168.174.4 266
192.168.174.255	255.255.255.255		在链路上	192.168.174.4 266
224.0.0.0	240.0.0.0		在链路上	127.0.0.1 306
224.0.0.0	240.0.0.0		在链路上	192.168.174.4 266
255.255.255.255	255.255.255.255		在链路上	127.0.0.1 306
255.255.255.255	255.255.255.255		在链路上	192.168.174.4 266

永久路由：

无

IPv6 路由表

活动路由：

如果跃点数	网络目标	网关
1	306 ::1/128	在链路上
11	266 fe80::/64	在链路上
11	266 fe80::cc02:583f:61e9:8f14/128	在链路上
1	306 ff00::/8	在链路上
11	266 ff00::/8	在链路上

永久路由：

```
arp-A
```



C:\Users\testuser>arp -a

接口: 192.168.174.4 --- 0xb		
Internet 地址	物理地址	类型
192.168.174.2	00-0c-29-dd-1d-9f	动态
192.168.174.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.252	01-00-5e-00-00-fc	静态

C:\Users\testuser>



#### 查询防火墙配置

关闭防火墙:

Windows Server 2003系统及以前版本, 命令如下:

```
netsh firewall setopmode disable
```

Windows server 2003之后系统版本, 命令如下:

```
netsh advfirewall setallprofiles state off
```

#### 查询防火墙配置

```
netsh firewall showconfig
```

C:\Users\testuser>netsh firewall show config

#### 域 配置文件配置(当前):

操作模式	= 禁用
例外模式	= 启用
多播/广播响应模式	= 启用
通知模式	= 禁用

#### 域 配置文件的允许的程序配置:

模式	流量方向	名称/程序
----	------	-------

#### 域 配置文件的端口配置:

端口	协议	流量方向	名称
----	----	------	----

#### 域 配置文件的 ICMP 配置:

模式	类型	描述
----	----	----

启用	2	允许出站数据包太大
----	---	-----------

#### 标准 配置文件配置:

操作模式	= 禁用
例外模式	= 启用
多播/广播响应模式	= 启用
通知模式	= 禁用

#### 标准 配置文件的允许的程序配置:

模式	流量方向	名称/程序
----	------	-------

#### 标准 配置文件的端口配置:

端口	协议	流量方向	名称
----	----	------	----



#### 修改防火墙配置

Windows Server 2003系统及之前版本, 允许指定程序全部链接, 命令如下:

```
netsh firewall addallowedprogram c:c.exe allow nc enable
```

[回到顶部](#)

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 addrule name="pass nc"dir=inaction=allow program="C: c.exe"

允许指定程序连出, 命令如下:  
netsh advfirewall firewall addrule name="Allow nc"dir=outaction=allow program="C: c.exe"

允许 3389 端口放行, 命令如下  
netsh advfirewall firewall addrule name="Remote Desktop"protocol=TCP dir=inlocalport=3389action=allow

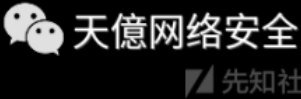
#####自定义防火墙日志存储位置  
netsh advfirewall setcurrentprofile loggingfilename "C:windowstempfw.log"

####查询远程连接服务  
#####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, 如下图所示:  
REG QUERY "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"/V PortNumber

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

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

C:\Users\testuser>
```



```
netsh advfirewall setcurrentprofile loggingfilename "C:windowstempfw.log"
netsh advfirewall firewall addrule name="Remote Desktop"protocol=TCP dir=inlocalport=3389action=allow
netsh advfirewall firewall addrule name="Remote Desktop"protocol=TCP dir=inlocalport=3389action=allow
netsh advfirewall firewall addrule name="Remote Desktop"protocol=TCP dir=inlocalport=3389action=allow
```

在Windows Server 2003中开启3389端口:  
方法一:  
查看开启的端口——没有开启3389端口

```
C:\Documents and Settings\Administrator>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING
TCP	192.168.174.169:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	0.0.0.0:1031	*:*	
UDP	0.0.0.0:1033	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1028	*:*	
UDP	127.0.0.1:1032	*:*	
UDP	192.168.174.169:123	*:*	
UDP	192.168.174.169:137	*:*	
UDP	192.168.174.169:138	*:*	



```
C:\Documents and Settings\Administrator>
```

执行语句:  
wmic RDToggle WHERE ServerName='%COMPUTERNAME%' callSetAllowTSConnections 1

执行结果:

```
C:\Documents and Settings\Administrator>wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
执行 C:\ADMIN-DDD8153C6\ROOT\CIMV2:Win32_TerminalServiceSetting.ServerName="ADMIN-DDD8153C6">->SetAllowTSConnections(<)
方法执行成功。
输出参数:
instance of __PARAMETERS
<
    ReturnValue = 0;
>;
```



先知社区

C:\Documents and Settings\Administrator>

成功开启3389端口:

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING
TCP	192.168.174.169:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	0.0.0.0:1031	*:*	
UDP	0.0.0.0:1033	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1028	*:*	
UDP	127.0.0.1:1034	*:*	
UDP	192.168.174.169:123	*:*	
UDP	192.168.174.169:137	*:*	
UDP	192.168.174.169:138	*:*	



C:\Documents and Settings\Administrator>

wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1

wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1

方法二:

查看开启端口——未开启3389:



C:\Documents and Settings\Administrator>netstat -an

# Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING
TCP	192.168.174.169:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	0.0.0.0:1031	*:*	
UDP	0.0.0.0:1033	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1028	*:*	
UDP	127.0.0.1:1034	*:*	
UDP	192.168.174.169:123	*:*	
UDP	192.168.174.169:137	*:*	
UDP	192.168.174.169:138	*:*	

C:\Documents and Settings\Administrator>

执行语句:

```
REGADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000/f
```

执行结果:

C:\Documents and Settings\Administrator>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f  
操作成功完成。

C:\Documents and Settings\Administrator>

查看端口开放情况——成功开启3389端口:

C:\Documents and Settings\Administrator&gt;netstat -ano

## Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	676
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	412
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1460
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING	1700
TCP	192.168.174.169:139	0.0.0.0:0	LISTENING	4
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		412
UDP	0.0.0.0:1026	*:*		732
UDP	0.0.0.0:1031	*:*		732
UDP	0.0.0.0:1033	*:*		732
UDP	0.0.0.0:4500	*:*		412
UDP	127.0.0.1:123	*:*		760
UDP	127.0.0.1:1028	*:*		760
UDP	127.0.0.1:1034	*:*		2252
UDP	192.168.174.169:123	*:*		760
UDP	192.168.174.169:137	*:*		4
UDP	192.168.174.169:138	*:*		4

C:\Documents and Settings\Administrator&gt;

在Windows Server 2008 和 Windows Server 2012 中开启 3389 端口

查看当前开发端口——未开放3389端口

C:\Windows\system32>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	696	
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	368	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	772	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	832	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	472	
TCP	0.0.0.0:64771	0.0.0.0:0	LISTENING	480	
TCP	0.0.0.0:64815	0.0.0.0:0	LISTENING	2440	
TCP	192.168.174.4:139	0.0.0.0:0	LISTENING	4	
TCP	:::135	:::0	LISTENING	696	
TCP	:::445	:::0	LISTENING	4	
TCP	:::47001	:::0	LISTENING	4	
TCP	:::49152	:::0	LISTENING	368	
TCP	:::49153	:::0	LISTENING	772	
TCP	:::49154	:::0	LISTENING	832	
TCP	:::49155	:::0	LISTENING	472	
TCP	:::64771	:::0	LISTENING	480	
TCP	:::64815	:::0	LISTENING	2440	
UDP	0.0.0.0:123	*:*		884	
UDP	0.0.0.0:500	*:*		832	
UDP	0.0.0.0:4500	*:*		832	
UDP	0.0.0.0:5355	*:*		1000	
UDP	127.0.0.1:58401	*:*		480	
UDP	127.0.0.1:58404	*:*		832	
UDP	127.0.0.1:65531	*:*		1600	
UDP	192.168.174.4:137	*:*		4	

之后执行如下命令来开启3389端口——管理员权限执行否则会报错

```
wmic /namespace:rootcimv2terminalservices path win32_terminalsettingsetting where (__CLASS != "") call setallowtsconnections 1
```

```
C:\Windows\system32>wmic /namespace:\\root\cimv2\terminalservices path win32_terminalsettingsetting where (__CLASS != "") call setallowtsconnections 1
Executing (\\WIN-SERVER-TEST\root\cimv2\terminalservices:Win32_TerminalServiceSetting.ServerName="WIN-SERVER-TEST")->setallowtsconnections()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
```

```
wmic /namespace:rootcimv2terminalservices path win32_tsgeneralsetting where (TerminalName='RDP-Tcp') call setuserauthenticationrequired 1
```

```
C:\Windows\system32>wmic /namespace:\\root\cimv2\terminalservices path win32_tsgeneralsetting where (TerminalName='RDP-Tcp') call setuserauthenticationrequired 1
Executing (\\WIN-SERVER-TEST\root\cimv2\terminalservices:Win32_TSGeneralSetting. TerminalName="RDP-Tcp")->setuserauthenticationrequired()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
};
```



```
regadd "HKLM\SYSTEM\CURRENT\CONTROLSET\CONTROL\TERMINAL SERVER" /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
```

```
C:\Windows\system32>reg add "HKLM\SYSTEM\CURRENT\CONTROLSET\CONTROL\TERMINAL SERVER" /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
操作成功完成。
```



```
REGADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal "Server" /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
```

之后成功开启3389端口:

```
C:\Windows\system32>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	696	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	2752	
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	368	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	772	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	832	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	472	
TCP	0.0.0.0:64771	0.0.0.0:0	LISTENING	480	
TCP	0.0.0.0:64815	0.0.0.0:0	LISTENING	2440	
TCP	192.168.174.4:139	0.0.0.0:0	LISTENING	4	
TCP	192.168.174.4:64875	192.168.174.2:135	ESTABLISHED	832	
TCP	192.168.174.4:64876	192.168.174.2:49158	ESTABLISHED	832	
TCP	192.168.174.4:64878	192.168.174.2:135	TIME_WAIT	0	
TCP	192.168.174.4:64879	192.168.174.2:49158	ESTABLISHED	480	
TCP	:::135	:::0	LISTENING	696	
TCP	:::445	:::0	LISTENING	4	
TCP	:::3389	:::0	LISTENING	2752	
TCP	:::47001	:::0	LISTENING	4	
TCP	:::49152	:::0	LISTENING	368	
TCP	:::49153	:::0	LISTENING	772	
TCP	:::49154	:::0	LISTENING	832	
TCP	:::49155	:::0	LISTENING	472	
TCP	:::64771	:::0	LISTENING	480	
TCP	:::64815	:::0	LISTENING	2440	
UDP	0.0.0.0:123	*:*		834	
UDP	0.0.0.0:500	*:*		832	
UDP	0.0.0.0:4500	*:*			



## 2、自动化信息收集

为了简化操作，我们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WindowsXP的低权限用户不能访问WMIC，Windows7以上版本允许低权限的用户访问WMIC并执行相关查询操作。

[回到顶部](#)

WMIC脚本的不载地址为[http://www.fuzzysecurity.com/scripts/files/wmic\\_info.rar](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，如下图所示：

Node	CSName	Description	ExecutablePath	ProcessId
WIN-SERVER-TEST	WIN-SERVER-TEST	System Idle Process		0
WIN-SERVER-TEST	WIN-SERVER-TEST	System		4
WIN-SERVER-TEST	WIN-SERVER-TEST	smss.exe		224
WIN-SERVER-TEST	WIN-SERVER-TEST	csrss.exe		316
WIN-SERVER-TEST	WIN-SERVER-TEST	wininit.exe		368
WIN-SERVER-TEST	WIN-SERVER-TEST	services.exe		472
WIN-SERVER-TEST	WIN-SERVER-TEST	lsass.exe		480
WIN-SERVER-TEST	WIN-SERVER-TEST	lsmon.exe		488
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		604
WIN-SERVER-TEST	WIN-SERVER-TEST	vmacthlp.exe		664
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		696
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		772
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		832
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		884
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		952
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		1000
WIN-SERVER-TEST	WIN-SERVER-TEST	svchost.exe		

### 3、Empire下主机信息收集

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，如下图所示：

```
(Empire: powershell/situational_awareness/host/winenum) > execute
(Empire: powershell/situational_awareness/host/winenum) >
Job started: KS6EBT

Username: Administrator

-----

AD Group Memberships

-----

Domain Users
Administrators
Schema Admins
Enterprise Admins
Domain Admins
Group Policy Creator Owners
```

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

### 三、查询当前权限

#### 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：

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

```
C:\Users\user>
```



天德网络安全

先知社区

本地管理员用户：当前权限为 win7-x64-test 本机的 administrator 用户：

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

```
C:\Users\Administrator>
```



天德网络安全

先知社区

域内用户：当前权限为 hacke 域内的 administrator 用户：

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

```
C:\Users\Administrator>
```



天德网络安全

先知社区

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 ntauthoritysystem 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。

### 获取域 SID

执行如下命令，获取域 SID：

```
whoami /all
```

可看到，当前域 hacke 的 SID 为 S-1-5-21-180313546-3823935851-3686928739，域用户 user1 的 SID 为 S-1-5-21-180313546-3823935851-3686928739-1106，如图 2-29 所示。

```
C:\Windows\system32\cmd.exe - whoami /all
```

```
C:\Users\testuser>whoami /all
```

用户信息

-----

用户名	SID
-----	-----

=====

hacke\testuser	S-1-5-21-180313546-3823935851-3686928739-1106
----------------	---



天德网络安全

先知社区

## 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：

### 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，如下图所示：

[回到顶部](#)

选定 C:\Windows\system32\cmd.exe

C:\Users\testuser>ipconfig /all

#### Windows IP 配置

```

主机名 . . . . . : win-server-test
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-29-24-C5-83
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
本地连接 IPv6 地址. . . . . : fe80::cc02:583f:61e9:8f14%11(首选)
IPv4 地址 . . . . . : 192.168.174.4(首选)
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . :
DHCPv6 IAID . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-25-44-7B-0E-00-0C-29-85-82-82
DNS 服务器 . . . . . : 192.168.174.2
TCP/IP 上的 NetBIOS . . . . . : 已启用

```

#### 隧道适配器 isatap.{72713B24-668C-4F4C-A3BD-65671104587B}:

```

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

```

#### 隧道适配器 本地连接\* 2:

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，如下图所示：

C:\Users\testuser>nslookup hacke.testlab

```

服务器:  UnKnown
Address:  192.168.174.2

```

```

名称:     hacke.testlab
Address:  192.168.174.2

```

C:\Users\testuser>\_

#### ###查看系统详细信息

执行如下命令，来查看系统信息，如结果所示，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

天億网络安全

天億网络安全

先知社区



```
BIOS 版本: Phoenix Technologies LTD 6.00, 2018/4/13
Windows 目录: C:\Windows
系统目录: C:\Windows\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (UTC+08:00)北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 2,047 MB
可用的物理内存: 1,578 MB
虚拟内存: 最大值: 4,095 MB
虚拟内存: 可用: 3,640 MB
虚拟内存: 使用中: 455 MB
页面文件位置: C:\pagefile.sys
域: hacke.testlab
登录服务器: \\DC
修补程序: 安装了 2 个修补程序。
[01]: KB2999226
[02]: KB976902
网卡: 安装了 1 个 NIC。
[01]: Intel(R) PRO/1000 MT Network Connection
连接名: 本地连接
启用 DHCP: 否
IP 地址
[01]: 192.168.174.4
[02]: fe80::cc02:583f:61e9:8f14
```



C:\Users\testuser>

###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:

```
nettime /domain
```

运行该命令后, 一般会有如下三种情况:

```
whoami /all
```

```
whoami /all
```

存在域, 但当前用户不是域用户, 提示说明权限不够, 如下图所示:

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

拒绝访问。



存在域, 并且当前用户是域用户, 如下图所示:

```
C:\Users\testuser>net time /domain
\\DC.hacke.testlab 的当前时间是 2020/2/14 13:35:45
命令成功完成。
```



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。



回到顶部

##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Namp等工具进行暴力扫描，也不要再在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。

###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。

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，如下图所示：

```
C:\Windows\System32\cmd.exe

C:\Users\testuser\Desktop>nbtscan-1.0.35.exe 192.168.174.0/20
192.168.174.1    WORKGROUP\DESKTOP-JEBLJJK    SHARING
192.168.174.2    HACKE\DC                      SHARING DC
192.168.174.3    HACKE\WIN7-TEST              SHARING
192.168.174.4    HACKE\WIN-SERVER-TEST        SHARING
*timeout (normal end of scan)

C:\Users\testuser\Desktop>
```

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，具体含义如下表所示：

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
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
EXECHANGE	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

###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，如下图所示：

```
for/L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.174.%I | findstr "TTL="

C:\Users\testuser\Desktop>for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.174.%I | findstr "TTL="
来自 192.168.174.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.174.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.174.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.174.4 的回复: 字节=32 时间<1ms TTL=128
```

也可以使用VBS脚本，代码如下：

```
strSubNet = "192.168.174."
SetobjFSO= CreateObject("Scripting.FileSystemObject")
SetobjJS = objFSO.CreateTextFile("C:\WindowsTempResult.txt")
Fori = 1To254
strComputer = strSubNet & i
blnResult = Ping(strComputer)
IfblnResult = TrueThen
objJS.WriteLine strComputer & " is alived ! :) "
EndIf
Next

objJS.Close
WScript.Echo "All Ping Scan , All Done ! :) "
FunctionPing(strComputer)
SetobjWMIService = GetObject("winmgmts:.rootcimv2")
SetcolItems = objWMIService.ExecQuery("Select * From Win32_PingStatus Where Address=' " & strComputer & " ")
ForEachobjItem IncolItems
SelectcaseobjItem.StatusCode
Case0
Ping = True
CaseElse
Ping = False
Endselect
ExitFor
Next
EndFunction
```

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


```
cscript:windowstempl.vbs
```

该命令默认会把扫描结果写到C:\Windows\Temp\Result.txt 文件中，相对而言速度很慢，不是很推荐，如下图所示：

```
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 ! :>
```



#### 四、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。


###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，如下图所示：

```
C:\Users\testuser>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\testuser>telnet DC 1433
正在连接DC...无法打开到主机的连接。 在端口 1433：连接失败

C:\Users\testuser>_
```



###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，如下图所示：

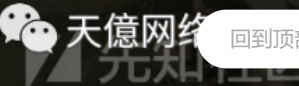
```
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  CONCURRENCY 10              yes       The number of concurrent ports to check per host
  DELAY       0               yes       The delay between connections, per thread, in milliseconds
  JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      192.168.174.2   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

msf5 auxiliary(scanner/portscan/tcp) > set ports 1-1024
ports => 1-1024
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.174.2
RHOSTS => 192.168.174.2
msf5 auxiliary(scanner/portscan/tcp) > set THREADS 10
THREADS => 10
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.174.2: - 192.168.174.2:53 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:88 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:135 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:139 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:389 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:445 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:464 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:593 - TCP OPEN
[+] 192.168.174.2: - 192.168.174.2:636 - TCP OPEN
[*] 192.168.174.2: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) > _
```



回到顶部

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。  
###PowerSploit的 Invoke-portscan.ps1  
PowerSploit中的Invoke-Portscan.ps1脚本，推荐使用无文件形式的扫描，如下图所示：  
Invoke-Portscan -Hosts 192.168.174.0/24 -T 4 -ports '445,1433,8080,3389,80' -oA c:\windowstempres.txt

PS C:\Users\testuser\Desktop\Test> ./Invoke-Portscan -Hosts 192.168.174.0/24 -T 4 -ports '445,1433,8080,3389,80' -oA c:\windowstempres.txt  
PS C:\Users\testuser\Desktop\Test>

磁盘 (C:) > Windows > Temp > 搜索 Temp

名称	修改日期	类型	大小
vmware-SYSTEM	2019/10/25 17:46	文件夹	
DMI8EE6.tmp	2019/10/25 17:38	TMP 文件	0 KB
log	2020/2/14 14:42	文本文档	2 KB
Result	2020/2/14 14:03	文本文档	1 KB
vmware-vmSvc	2020/2/14 9:15	文本文档	34 KB
vmware-vmusr	2020/2/13 23:38	文本文档	12 KB
vmware-vmvss	2020/2/13 23:39	文本文档	1 KB

Result - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

192.168.174.1 is alived ! :)  
192.168.174.2 is alived ! :)  
192.168.174.3 is alived ! :)  
192.168.174.4 is alived ! :)

Invoke-Portscan -Hosts 192.168.174.0/24 -T 4 -ports '445,1433,8080,3389,80' -oA c:\windowstempres.txt

五、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 权限用户可以运行以下查询命令）。

1、查询域

查询域的命令如下：

net view/domain

C:\Users\testuser>net view /domain  
Domain  
  
-----  
HACKE  
命令成功完成。  
  
C:\Users\testuser>\_

天億网络安全  
先知社区

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，如下图所示。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，"filesrv"可能是文件服务器等。

net view/domain:XXX

```
C:\Users\testuser>net view /domain:hacke
服务器名称      注解
```

```
-----
\\DC
\\WIN-SERVER-TEST
\\WIN7-TEST
命令成功完成。
```



```
C:\Users\testuser>
```

### 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：

```
net group/domain
```

```
C:\Users\testuser>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。
```

```
C:\Users\testuser>_
```



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。

### 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：

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



```
C:\Users\testuser>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

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

```
C:\Users\testuser>
```



## 5. 获取域信任列表

执行如下命令，获取域信任列表信息：

```
nltest/domain_trusts
```

```
C:\Users\testuser>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
```



```
C:\Users\testuser>
```

## 六、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

```
nltest/DCLIST:xxx
```

```
C:\Users\testuser>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
```

```
C:\Users\testuser>_
```



### 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:

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

```
C:\Users\testuser>Nslookup -type=SRV _ldap._tcp
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 192.168.174.2

_ldap._tcp.hacke.testlab SRV service location:
        priority = 0
        weight = 100
        port = 389
        svr hostname = dc.hacke.testlab
dc.hacke.testlab internet address = 192.168.174.2
```

```
C:\Users\testuser>
```



### 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：

```
nettime /domain
```

```
C:\Users\testuser>net time /domain
\\DC.hacke.testlab 的当前时间是 2020/2/14 16:48:46
```

命令成功完成。

```
C:\Users\testuser>
```



#### 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：

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

```
C:\Users\testuser>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。
```

```
C:\Users\testuser>
```



## 七、定位域管理员

### 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。

### 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。

### 3. 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，其原理是通过检查注册表里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，如下图所示：

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



```
C:\Windows\System32\cmd.exe
```

```
Microsoft Windows [版本 6.1.7601]
```

```
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
```

```
C:\Users\testuser\Desktop\PSTools>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:
```

```
<unknown time> HACKE\Administrator
```

```
Users logged on via resource shares:
```

```
2020/2/14 21:27:22 HACKE\testuser
```

```
C:\Users\testuser\Desktop\PSTools>
```



-: 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。

#### 4. pveFindADUser

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，如下图所示：

```
pveFindADUser.exe<参数>
```

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

```
PVE 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>
```

```
[+] Report written to report.csv
```



-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 (DOMAINUsername)，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 (DOMAINUsername)，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。

#### 5. netview

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

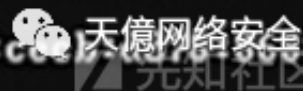
下命令及参数，如下图所示：

```
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
```



-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。


PS:其他的就不再赘述和演示了，有兴趣的可以自我使用看看~

## 八、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”，如下图所示：

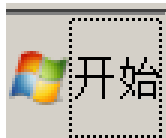
- Windows PowerShell
- Windows PowerShell (x86)
- Windows PowerShell Modules

 查看更多结果

powershel



注销



天园网络安全

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，如下图所示：

## Windows PowerShell

版权所有 (C) 2009 Microsoft Corporation。保留所有权利。

```
PS C:\Windows\system32> _
```



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，如下图所示：

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



将 PowerShell 执行权限改为 Unrestricted，输入“Y”，如下所示：

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

### 执行策略更改

执行策略可以防止您执行不信任的脚本。更改执行策略可能会使您面临 [about\\_Execution\\_Policies](#) 帮助主题中所述的安全风险。是否要更改执行策略？

[Y] 是(Y) [N] 否(N) [S] 挂起(S) [?] 帮助 (默认值为“Y”)：Y

```
PS C:\Windows\system32> _
```



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，如下图所示：

```
PS C:\Users\testuser\Desktop\PowerSploit-master> cd .\Recon
PS C:\Users\testuser\Desktop\PowerSploit-master\Recon> Import-Module .\PowerView.ps1
PS C:\Users\testuser\Desktop\PowerSploit-master\Recon> _
```



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。

PS：PowerShell在内网渗透中还是很有用的，由于相关的内容过多就不再展开了~

## 九、总结

由于文章篇幅原因，这里不再多赘述其他内容了，至于内网渗透中信息收集的方法自然不仅仅局限于上面这些，有兴趣的可以做深入的了解与分析，同时GitHub上也有很多关于内网信息收集的方法与辅助脚本~

相关参考

《内网安全攻防》

《Metasploit渗透测试指南》

《PowerShell实战指南第三版》

「天億网络安全」知识星球一个网络安全学习的星球！星球主要分享、整理、原创编辑等网络安全相关学习资料，一个真实有料的网络安全学习平台，大家共同学习、共同进步！

知识星球定价：199元/年，（服务时间为一年，自加入日期顺延一年）。

如何加入：扫描下方二维码，扫码付费即可加入。

加入知识星球的同学，请加我微信，拉您进VIP交流群！

回到顶部