常用收集域信息命令

```
Net use
Net view
Tasklist /v
Ipconfig /all
net group /domain 获得所有域用户组列表
net group “domain admins” /domain 获得域管理员列表
net group “enterprise admins” /domain 获得企业管理员列表
net localgroup administrators /domain 获取域内置administrators组用户（enterprise admins、domain admins）
net group “domain controllers” /domain 获得域控制器列表
net group “domain computers” /domain 获得所有域成员计算机列表
net user /domain 获得所有域用户列表
net user someuser /domain 获得指定账户someuser的详细信息
net accounts /domain 获得域密码策略设置，密码长短，错误锁定等信息
nltest /domain_trusts 获取域信任信息
```


SPN扫描

不同于常规的tcp/udp端口扫描，由于spn本质就是正常的Kerberos请求，所以扫描是非常隐蔽，日前针对此类扫描的检测暂时也比较少。

大部分win系统默认已自带spn探测工具即：`setspn.exe`

此操作无需管理权限

域内机器执行

```
setspn -T target.com -Q */*
```

可完整查出当前域内所有spn。

```
Checking domain DC=rootkit,DC=org
CN=OWA2013,OU=Domain Controllers,DC=rootkit,DC=org
    IMAP/OWA2013
    IMAP/OWA2013.rootkit.org
    IMAP4/OWA2013
    IMAP4/OWA2013.rootkit.org
    POP/OWA2013
    POP/OWA2013.rootkit.org
    POP3/OWA2013
    POP3/OWA2013.rootkit.org
    exchangeRFR/OWA2013
    exchangeRFR/OWA2013.rootkit.org
    exchangeMDB/OWA2013
    exchangeMDB/OWA2013.rootkit.org
    SMTP/OWA2013
    SMTP/OWA2013.rootkit.org
    SmtpSvc/OWA2013
    SmtpSvc/OWA2013.rootkit.org
    exchangeAB/OWA2013
```

```
    exchangeAB/OWA2013.rootkit.org
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/OWA2013.rootkit.org
    ldap/OWA2013.rootkit.org/ForestDnsZones.rootkit.org
    ldap/OWA2013.rootkit.org/DomainDnsZones.rootkit.org
    TERMSRV/OWA2013
    TERMSRV/OWA2013.rootkit.org
    DNS/OWA2013.rootkit.org
    GC/OWA2013.rootkit.org/rootkit.org
    RestrictedKrbHost/OWA2013.rootkit.org
    RestrictedKrbHost/OWA2013
    RPC/58650e64-9681-4c62-b26e-7914b9041f72._msdcs.rootkit.org
    HOST/OWA2013/ROOTKIT
    HOST/OWA2013.rootkit.org/ROOTKIT
    HOST/OWA2013
    HOST/OWA2013.rootkit.org
    HOST/OWA2013.rootkit.org/rootkit.org
    E3514235-4B06-11D1-AB04-00C04FC2DCD2/58650e64-9681-4c62-b26e-
7914b9041f72/rootkit.org
    ldap/OWA2013/ROOTKIT
    ldap/58650e64-9681-4c62-b26e-7914b9041f72._msdcs.rootkit.org
    ldap/OWA2013.rootkit.org/ROOTKIT
    ldap/OWA2013
    ldap/OWA2013.rootkit.org
    ldap/OWA2013.rootkit.org/rootkit.org
CN=krbtgt,CN=Users,DC=rootkit,DC=org
    kadmin/changepw
CN=dbadmin,OU=运维部,DC=rootkit,DC=org
    MSSQLSvc/Srv-Web-Kit.rootkit.org:1433
    MSSQLSvc/Srv-Web-Kit.rootkit.org
CN=SRV-WEB-KIT,CN=Computers,DC=rootkit,DC=org
    TERMSRV/SRV-WEB-KIT
    TERMSRV/Srv-Web-Kit.rootkit.org
    WSMAN/Srv-Web-Kit
    WSMAN/Srv-Web-Kit.rootkit.org
    RestrictedKrbHost/SRV-WEB-KIT
    HOST/SRV-WEB-KIT
    RestrictedKrbHost/Srv-Web-Kit.rootkit.org
    HOST/Srv-Web-Kit.rootkit.org
CN=PC-JERRY-KIT,CN=Computers,DC=rootkit,DC=org
    RestrictedKrbHost/PC-JERRY-KIT
    HOST/PC-JERRY-KIT
    RestrictedKrbHost/PC-jerry-Kit.rootkit.org
    HOST/PC-jerry-Kit.rootkit.org
CN=PC-MICLE-KIT,CN=Computers,DC=rootkit,DC=org
    RestrictedKrbHost/PC-MICLE-KIT
    HOST/PC-MICLE-KIT
    RestrictedKrbHost/PC-micle-Kit.rootkit.org
    HOST/PC-micle-Kit.rootkit.org
CN=PC-TORNDO-KIT,CN=Computers,DC=rootkit,DC=org
    HOST/PC-TORNDO-KIT
    HOST/pc-torndo-Kit.rootkit.org
CN=sqladmin,OU=运维部,DC=rootkit,DC=org
    variant/golden

Existing SPN found!
```

定位域控

查询dns解析记录

若当前主机的dns为域内dns，可通过查询dns解析记录定位域控。

```
nslookup -type=all _ldap._tcp.dc._msdcs.rootkit.org
```

```
C:\Users\sqladmin\Desktop>nslookup -type=all _ldap._tcp.dc._msdcs.rootkit.org
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.3.144

_ldap._tcp.dc._msdcs.rootkit.org        SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = owa2013.rootkit.org
owa2013.rootkit.org     internet address = 192.168.3.144

C:\Users\sqladmin\Desktop>
```


SPN扫描

在SPN扫描结果中可以通过`CN=OWA2013,OU=Domain Controllers,DC=rootkit,DC=org`来进行域控的定位。

net group

```
net group "domain controllers" /domain
```

```
C:\Users\sqladmin\Desktop>net group "domain controllers" /domain
The request will be processed at a domain controller for domain rootkit.org.

Group name     Domain Controllers
Comment        域中所有域控制器

Members

-------------------------------------------------------------------------------
OWA2013$
The command completed successfully.
```

端口识别

扫描内网中同时开放389和53端口的机器。

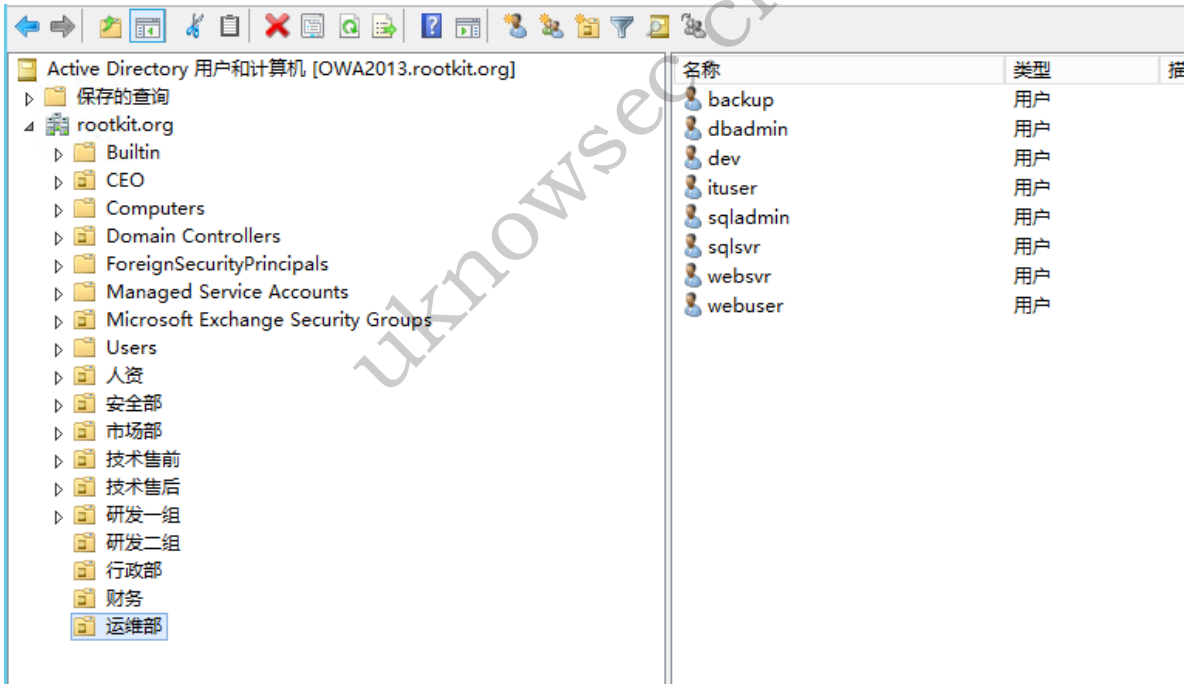
端口：389
服务：LDAP、ILS
说明：轻型目录访问协议和NetMeeting Internet Locator Server共用这一端口。

端口：53
服务：Domain Name Server（DNS）
说明：53端口为DNS(Domain Name Server，域名服务器)服务器所开放，主要用于域名解析，DNS服务在NT系统中使用的最为广泛。通过DNS服务器可以实现域名与IP地址之间的转换，只要记住域名就可以快速访问网站。

```
TCP    169.254.96.200:59201   169.254.96.200:444     TIME_WAIT       0
TCP    192.168.3.144:53       0.0.0.0:0              LISTENING       1848
TCP    192.168.3.144:139      0.0.0.0:0              LISTENING       4
TCP    192.168.3.144:389      192.168.3.144:13038    ESTABLISHED     552
```

域内关键组

比如在拿到域控后可以通过重点关注关键部门人员的机器来得到更多的信息。



以上图为例，我们可以重点关注和监控运维部的用户机器，通常他们的机器上存在大量内网网络拓扑和网络构架信息或者是一些重要的密码本。

AdFind

C++实现(未开源)，用于查询域内信息

http://www.joeware.net/freetools/tools/adfind/index.htm

常用命令如下：

列出域控制器名称：

```
AdFind -sc dclist
```

查询当前域中在线的计算机：

```
AdFind -sc computers_active
```

查询当前域中在线的计算机(只显示名称和操作系统):

```
AdFind -sc computers_active name operatingSystem
```

查询当前域中所有计算机:

```
AdFind -f "objectcategory=computer"
```

查询当前域中所有计算机(只显示名称和操作系统):

```
AdFind -f "objectcategory=computer" name operatingSystem
```

查询域内所有用户:

```
AdFind -users name
```

查询所有GPO:

```
AdFind -sc gpodmp
```