

# PENTEST ACTIVE DIRECTORY ROCKS!



25 junio 14-16h Donostia

Nacho Brihuega a.k.a n4xh4ck5

## Contenido

Requisitos y recursos.....	4
Configuración del laboratorio .....	5
Configuración de red .....	5
Configuración del controlador de dominio (DC) .....	5
Configuración Workstation y SRV .....	6
Configuración del directorio activo .....	7
Generación del AD .....	7
Unir máquinas al DC.....	8
Unir máquina Workstation.....	8
Unir máquina SRV.....	12
Configuraciones de seguridad.....	16
Configuración CLM (Constrained Language Mode) .....	16
Configuración AppLocker .....	18
Configuración AMSI.....	21
Generación tráfico.....	22
Referencias.....	23

## Tabla de ilustraciones

Ilustración 1. Creación red interna.....	5
Ilustración 2. Asignación rango red internal .....	5
Ilustración 3. Adicción red internal al DC.....	6
Ilustración 4. Esquema VM laboratorio .....	6
Ilustración 5. Creación del dominio .....	7
Ilustración 6. Generación del contenido en AD .....	8
Ilustración 7. Comprobación IP Workstation .....	8
Ilustración 8. Configuración DNS.....	9
Ilustración 9. Proceso de anexión de WK a brihuega.local .....	10
Ilustración 10. Proceso de unión WK a brihuega.local.....	11
Ilustración 11. Proceso de unión WK a brihuega.local.....	11
Ilustración 12. Anexión WK a brihuega.local.....	12
Ilustración 13. Revisión en el DC de WK incluido.....	12
Ilustración 14. Comprobación IP en SRV .....	13
Ilustración 15. Configuración DNS en SRV .....	13
Ilustración 16. Introducción SRV al dominio brihuega.local .....	14
Ilustración 17. Introducción SRV al dominio brihuega.local .....	14
Ilustración 18. Anexión de SRV al dominio brihuega.local.....	15
Ilustración 19. Anexión SRV al dominio brihuega.local.....	15
Ilustración 20. Comprobación en el DC la inclusión de SRV.....	15
Ilustración 21. Full language por defecto.....	16
Ilustración 22. Configuración CLM como variable de entorno .....	16
Ilustración 23. Adición CLM como variable de entorno.....	17
Ilustración 24. CLM configurado .....	17
Ilustración 25. Testeo CLM.....	17
Ilustración 26. CLM mediante registro.....	18
Ilustración 27. Configuración AppLocker .....	18
Ilustración 28. Configuración AppLocker .....	19
Ilustración 29. Arrancado el servicio Application identity .....	19
Ilustración 30. Comprobación servicio application identity.....	20
Ilustración 31. Bloqueo script por Applocker.....	20
Ilustración 32. Comprobación AMSI habilitado .....	21

## Requisitos y recursos

- **Requisitos:**
  - Software de virtualización. En este caso se ha usado Oracle Virtual Box.
  - 3 máquinas virtuales:
    - 1 DC – Controlador de dominio Windows Server 2019
    - 1 servidor (SRV) – Servidor Windows Server 2019
    - 1 workstation – Cliente Windows 10
  - Se recomienda que el equipo anfitrión donde se monte el laboratorio tenga suficiente capacidad de memoria RAM. Al menos 16 GB.
- **Recursos necesarios**
  - Scripts de automatización para generación AD:  
<https://github.com/dievus/ADGenerator>
  - ISO de sistemas operativos Windows:
    - <https://www.microsoft.com/es-es/software-download/windows10>
    - <https://www.microsoft.com/es-es/evalcenter/download-windows-server-2019>

## Configuración del laboratorio

### Configuración de red

Se crea una red llamada “Internal”. Para ello, desde el menú principal en preferencias-red:

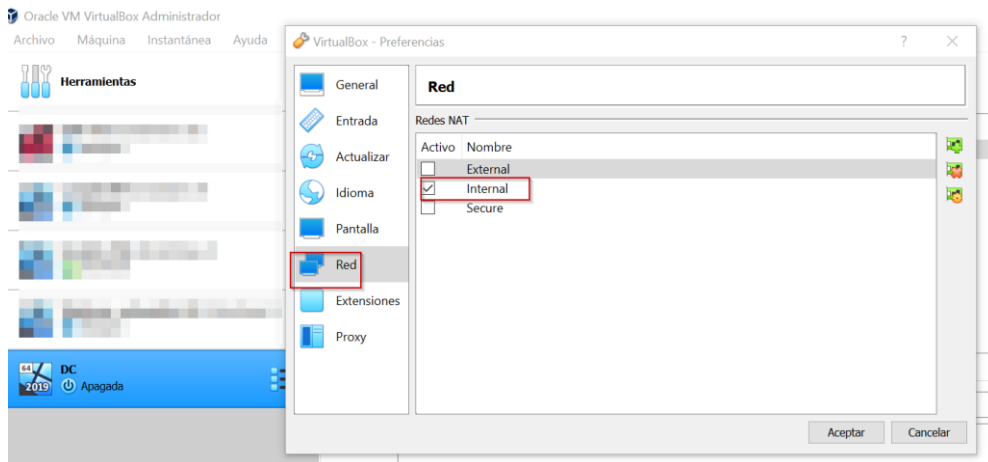


Ilustración 1. Creación red interna

Y se asigna un rango:

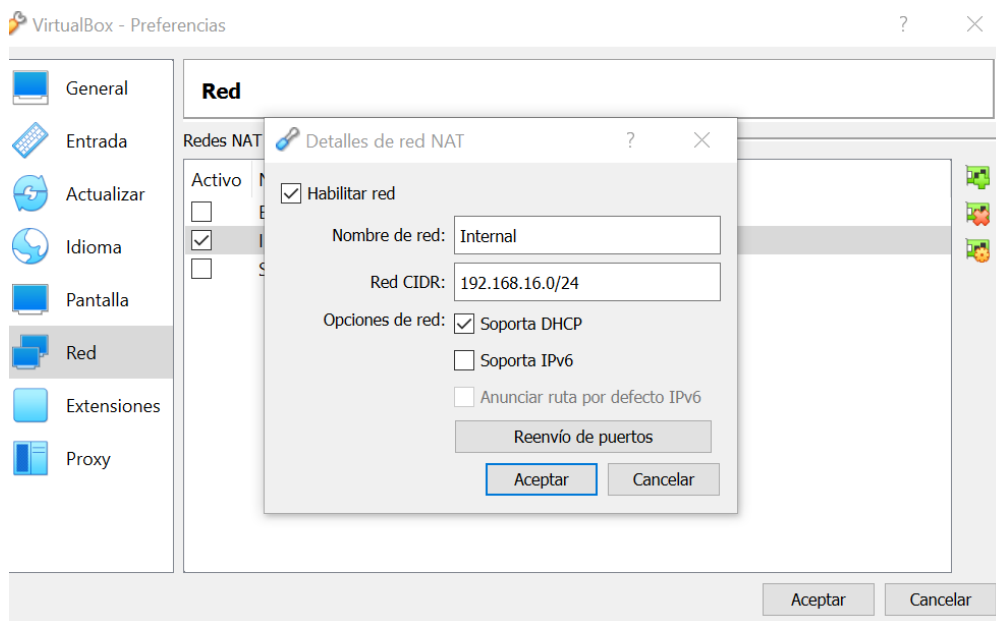


Ilustración 2. Asignación rango red internal

### Configuración del controlador de dominio (DC)

Se crea la máquina y se añade la iso de windows server 2019. Todo Next. Una vez creada, se asigna la red interna que se ha creado anteriormente:

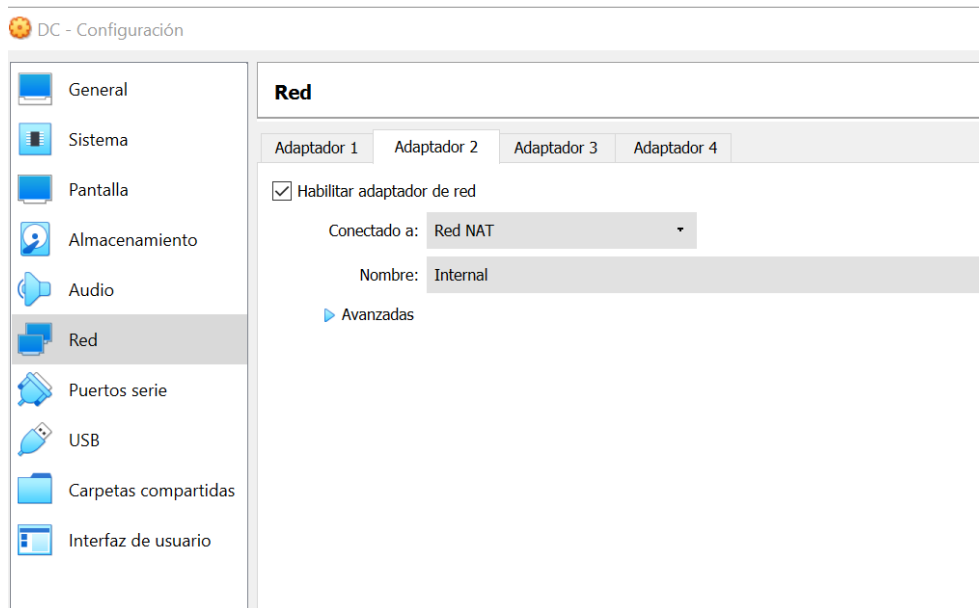


Ilustración 3. Adición red internal al DC

## Configuración Workstation y SRV

Se crea la máquina. Next, Next y se toman 20 GB de disco duro. Se configuran las interfaces de red: Nat y Red NAT internal.

En el caso del Workstation se selecciona la iso de Windows 10, mientras para el SRV el Windows Server 2019.

El resultado del laboratorio sería algo así:

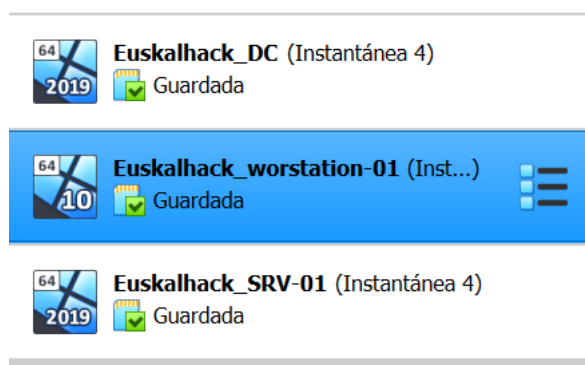


Ilustración 4. Esquema VM laboratorio

## Configuración del directorio activo

### Generación del AD

Se parte desde la máquina del DC. Para automatizar el proceso, se utilizará este script:

<https://github.com/dievus/ADGenerator>

En primer lugar, se creará el dominio. En este caso, lo he llamado “brihuega.local”. Aquí el asistente podrá poner el nombre que desee. Se recomienda usar la ISO del SSOO en inglés para evitar posibles problemas

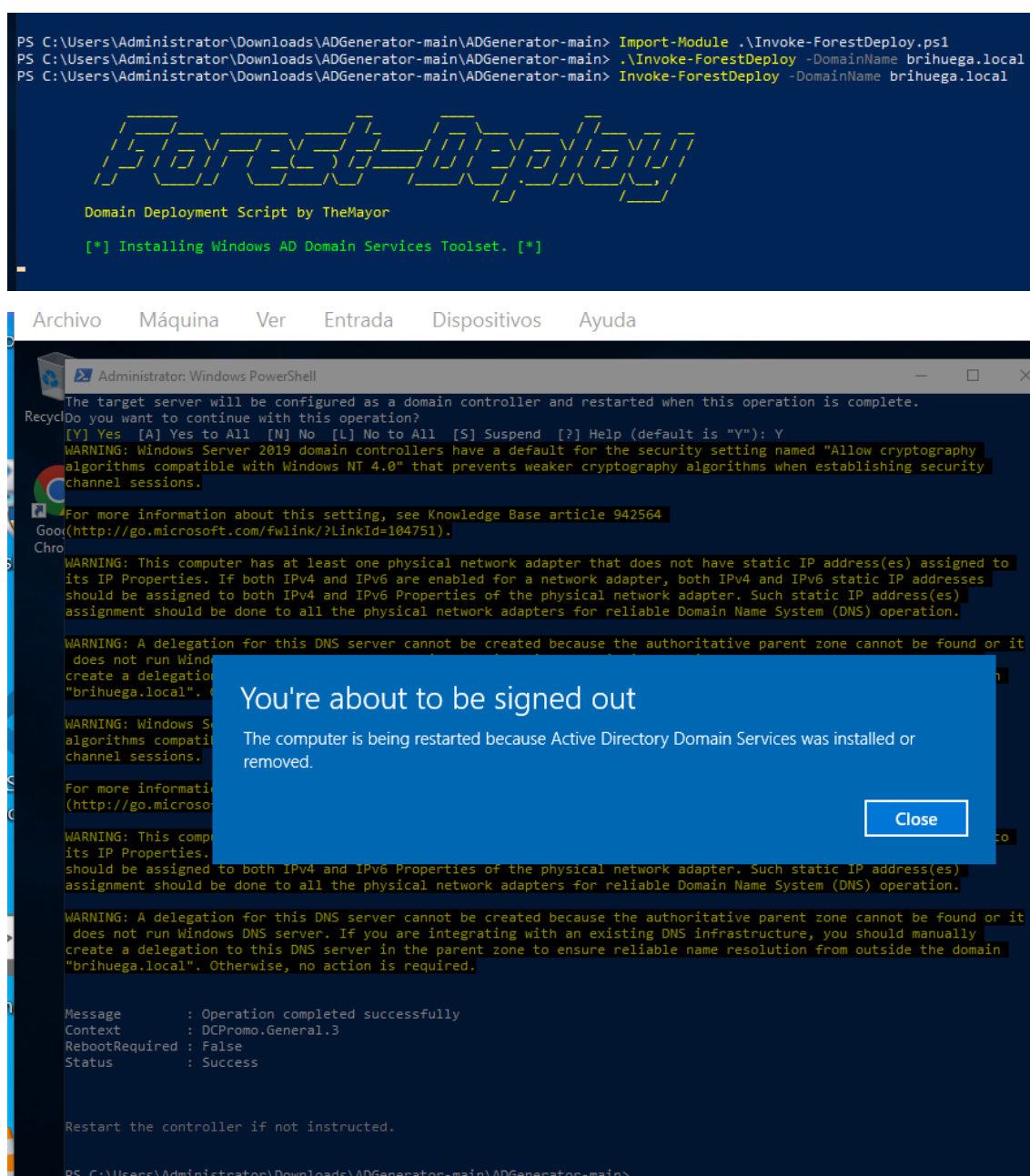


Ilustración 5. Creación del dominio

Una vez finalizado, se hará un signout.

Llegados a este punto, se recomienda crear un snapshot con objeto de volver a este punto por si algo fallará en los siguientes pasos.

A continuación, tras hacer login de nuevo, hay que editar el fichero ADGenerator.ps1 cambiando el nombre del dominio que desee el estudiante. En mi caso, será cambiar “mayor” por “brihuega”.

Seguidamente, desde una consola de powershell con permisos de admin:

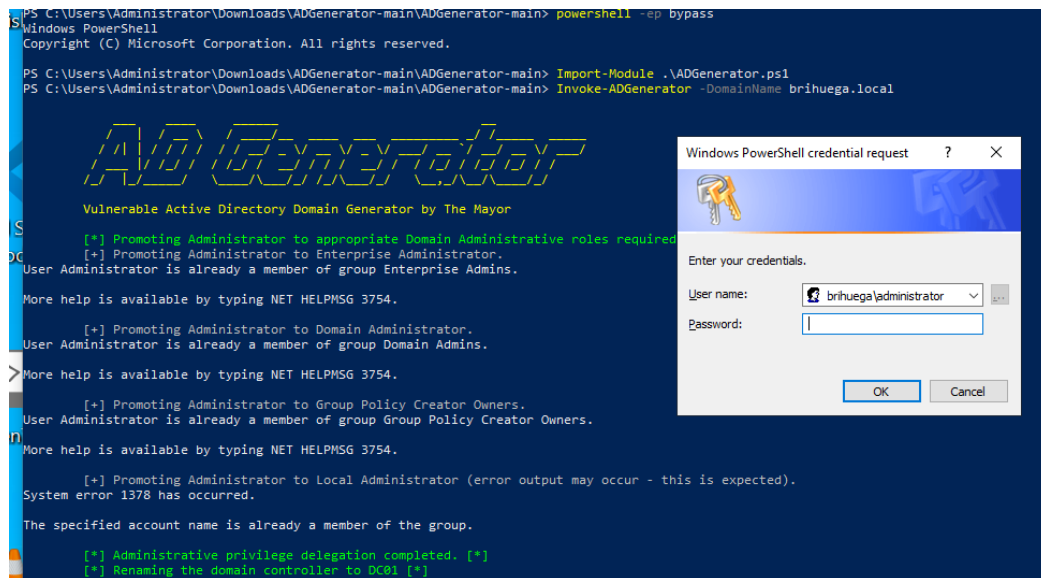


Ilustración 6. Generación del contenido en AD

## Unir máquinas al DC

Una vez creado el dominio y promocionado el servidor de la máquina que hemos llamado DC a controlador de dominio.

## Unir máquina Workstation

Comprobamos que tenemos la IP de la red internal:

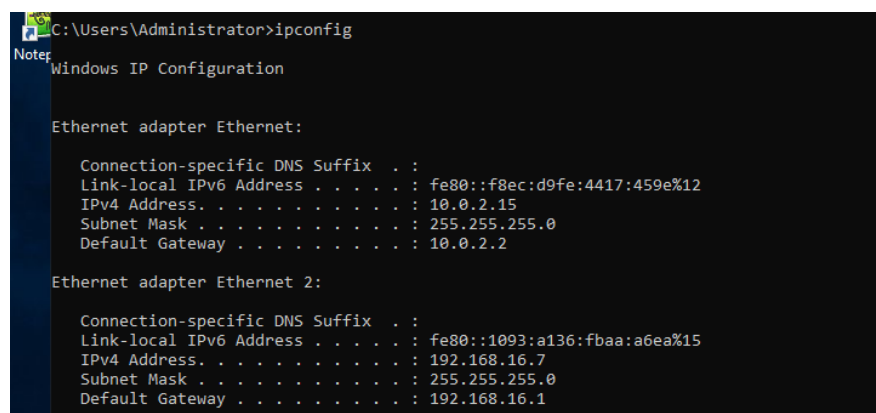
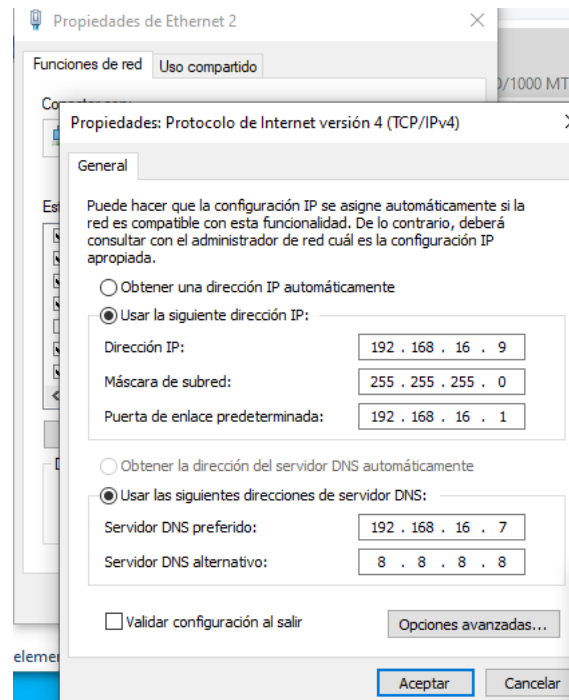


Ilustración 7. Comprobación IP Workstation

A continuación, se configura el DNS:





*Ilustración 8. Configuración DNS*

En el caso que diera error al acceder, se recomienda seguir este post:  
<https://www.analysisman.com/2021/04/windows-server-gpedit.html>

A continuación, se incluye en el dominio. Para ello, se siguen estos pasos:

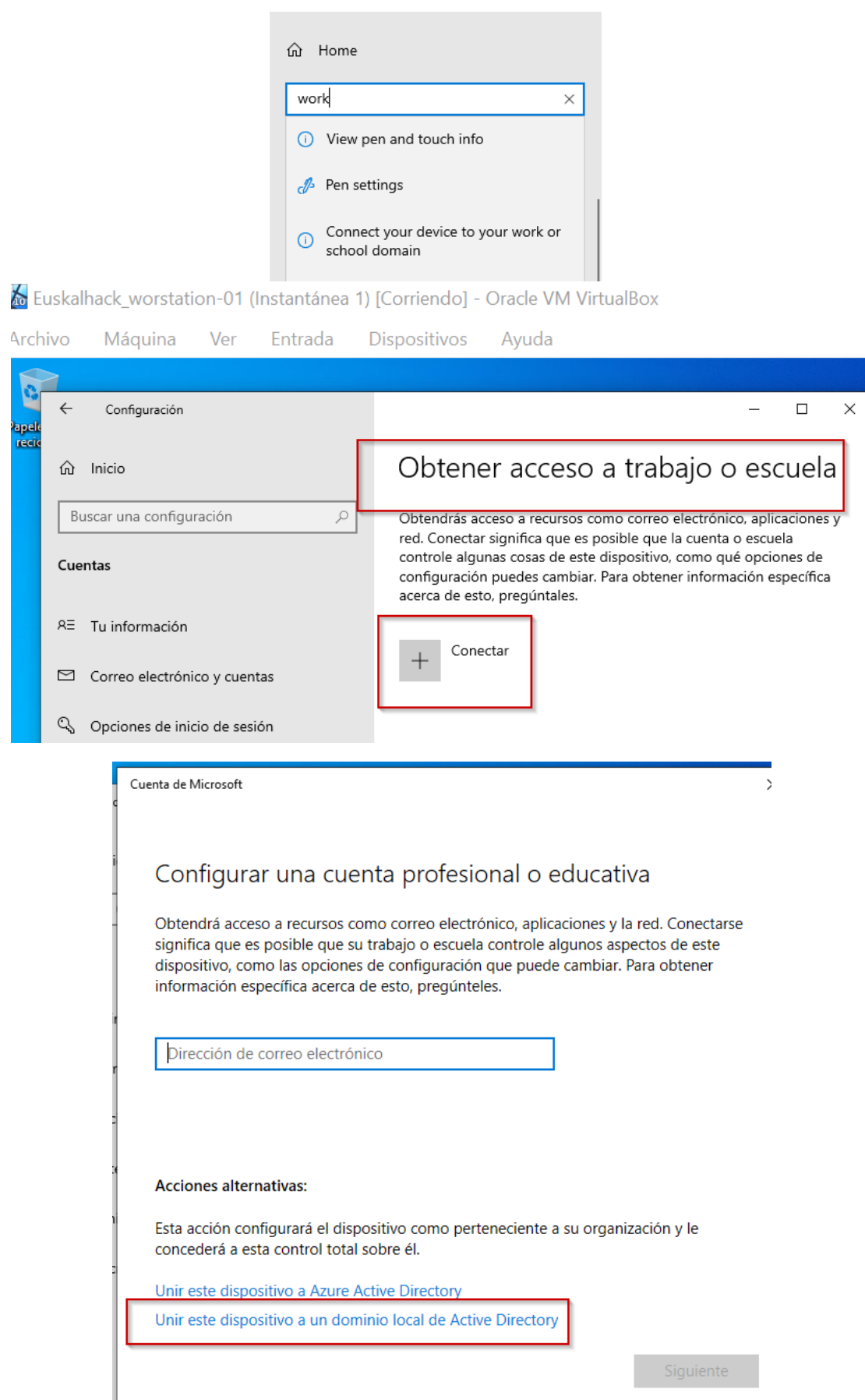


Ilustración 9. Proceso de anexión de WK a brihuega.local

Se introducen el nombre del dominio: brihuega.local

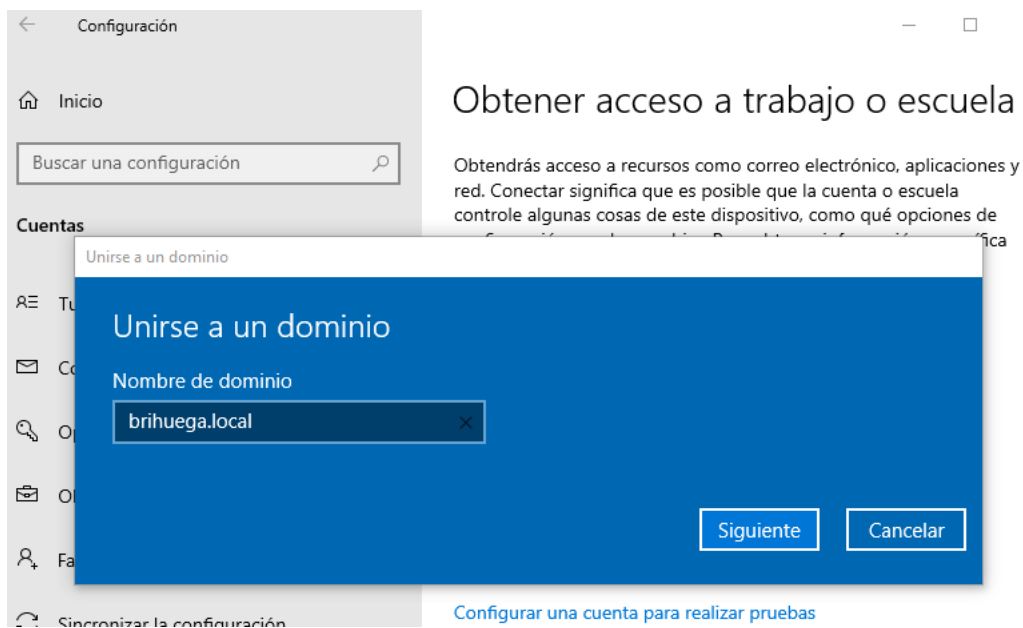


Ilustración 10. Proceso de unión WK a brihuega.local

Se introducen las siguientes credenciales de un usuario del dominio (fue creado en el script utilizado inicialmente):

m.seitz:Phi11i35@44

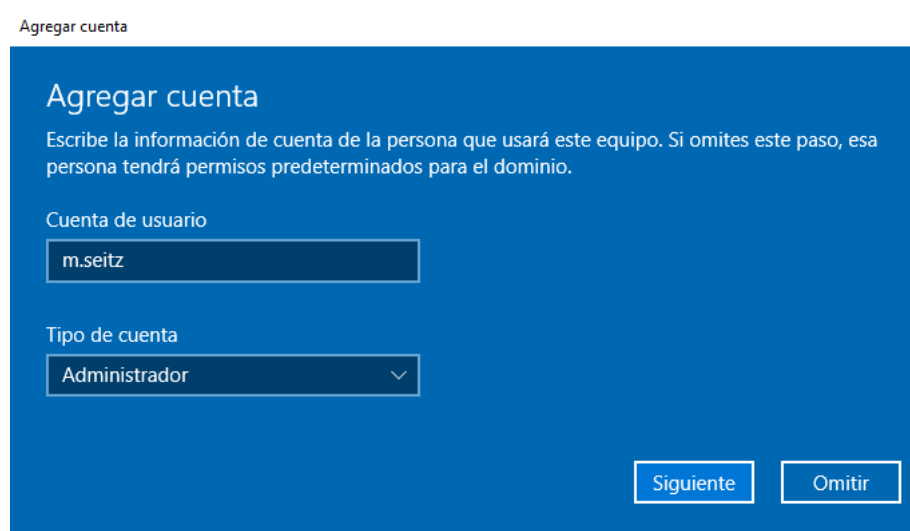


Ilustración 11. Proceso de unión WK a brihuega.local

Se reinicia:

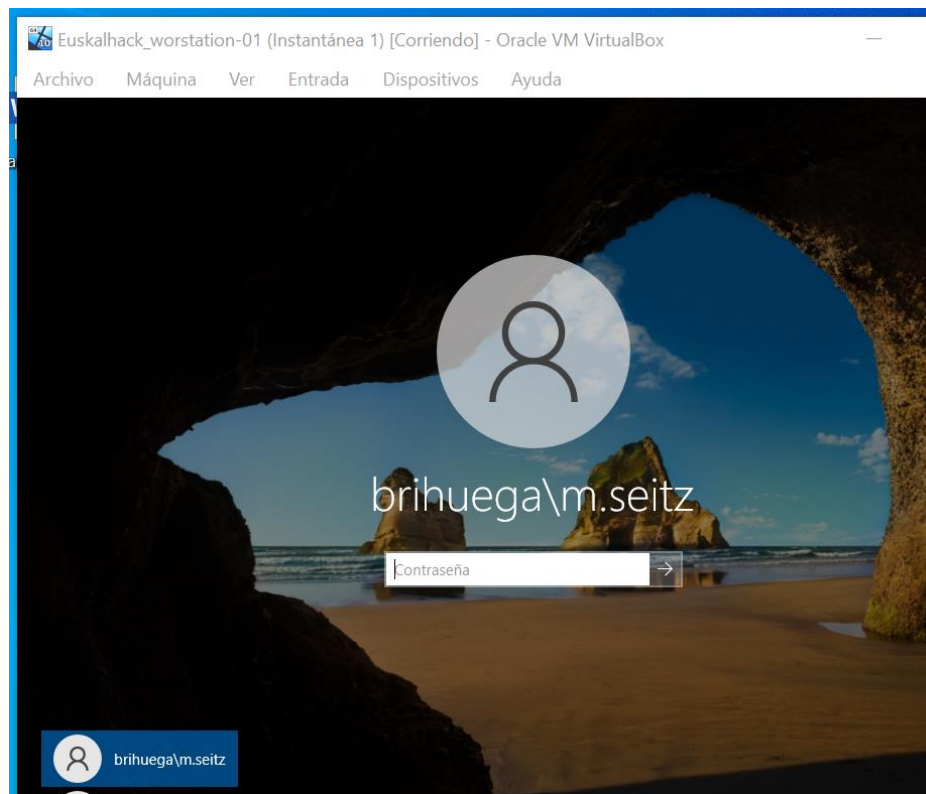


Ilustración 12. Anexión WK a brihuega.local

Tras loguearse, se puede revisar que ya está reflejado en el DC:

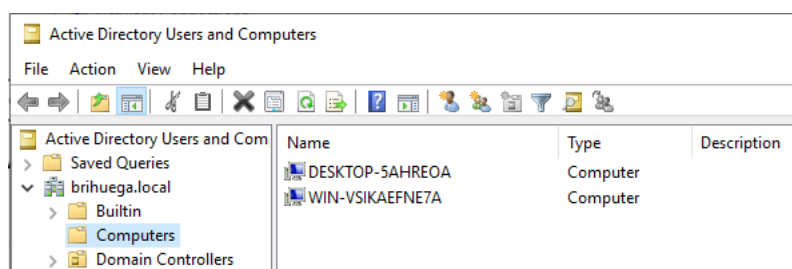


Ilustración 13. Revisión en el DC de WK incluido

Unir máquina SRV

Análogamente para el SRV se accede con un usuario administrador local y se comprueba la IP:

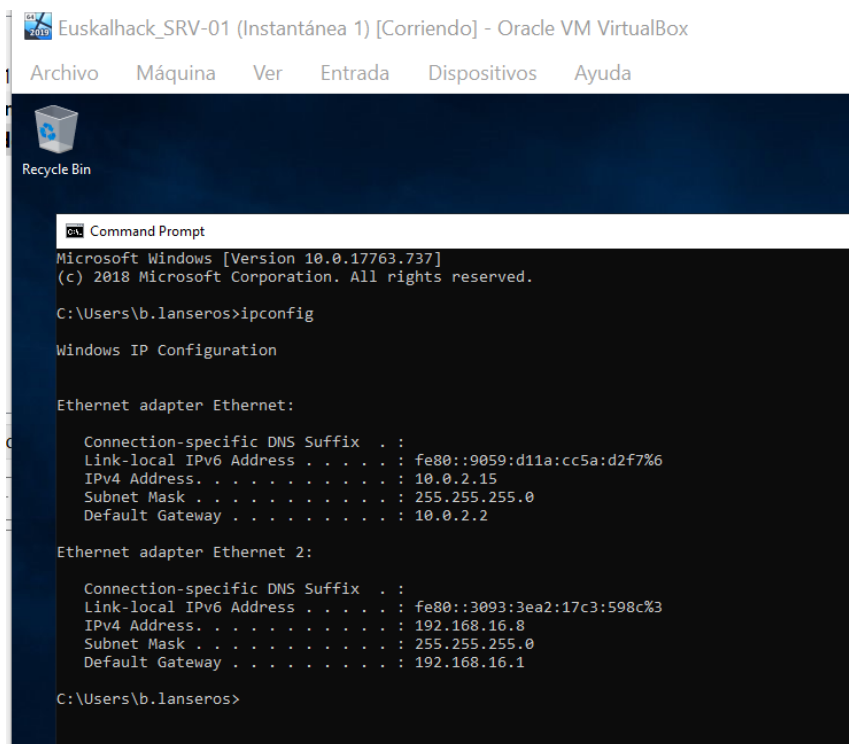


Ilustración 14. Comprobación IP en SRV

Se configura el DNS:

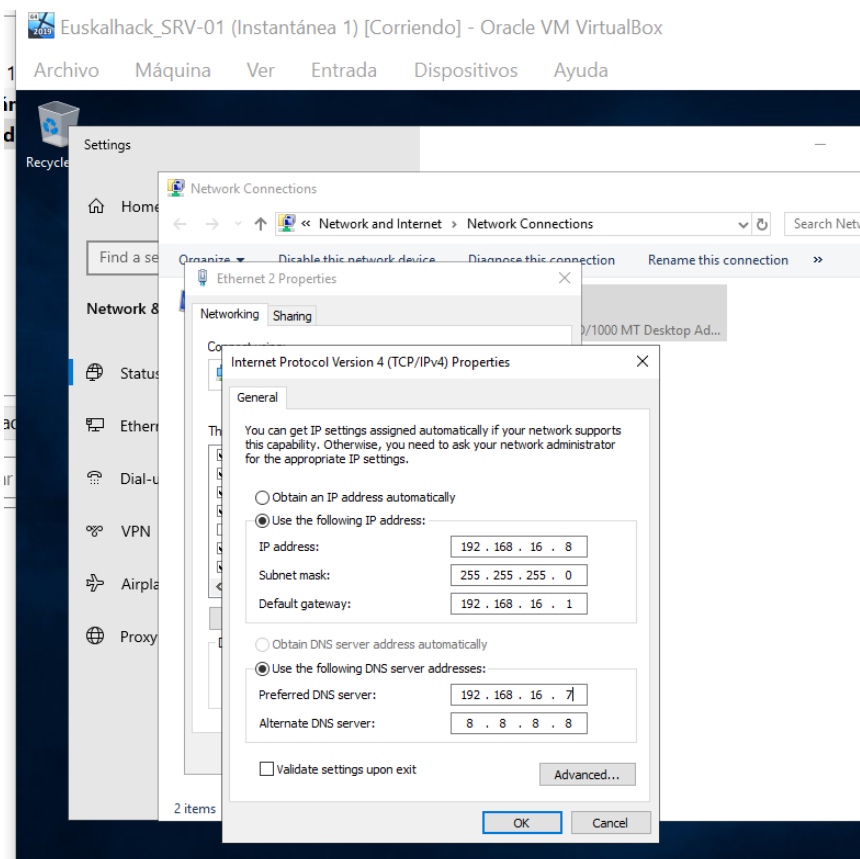


Ilustración 15. Configuración DNS en SRV

Seguidamente, se une al dominio. Para ello, se siguen los siguientes pasos:

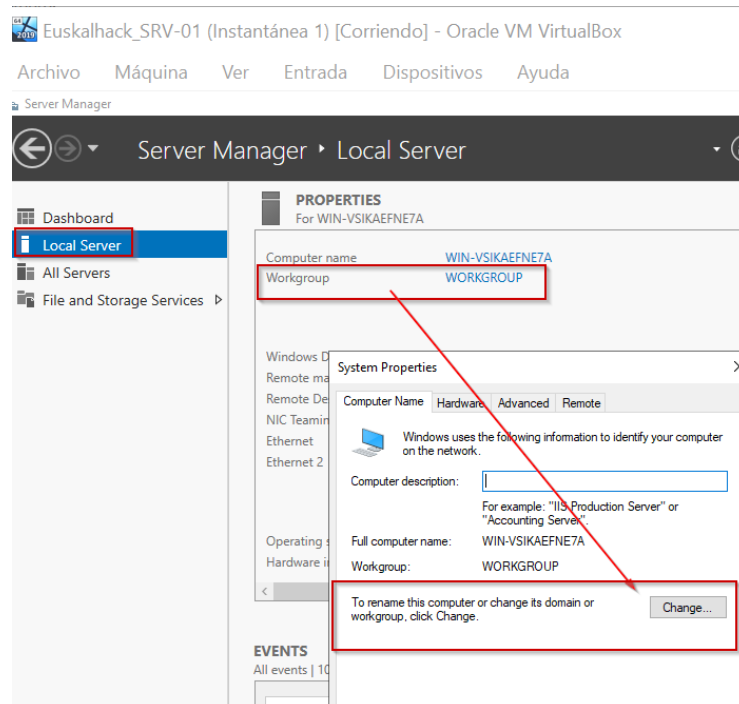


Ilustración 16. Introducción SRV al dominio brihuega.local

Se introduce el domain: brihuega.local

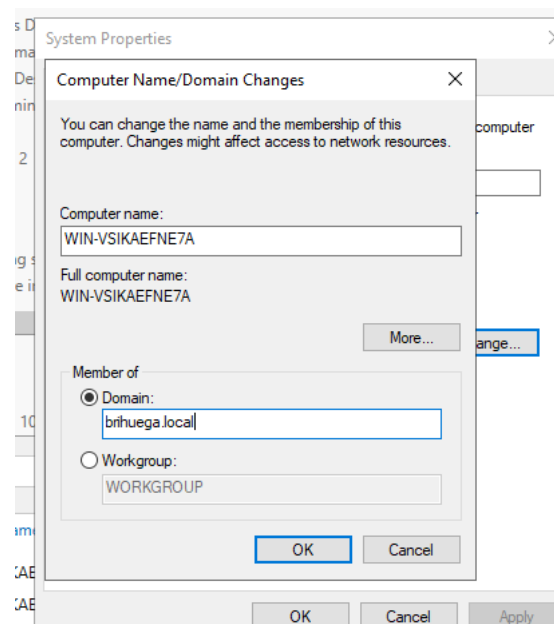


Ilustración 17. Introducción SRV al dominio brihuega.local

Piden las credenciales, en las que hay que meter las siguientes de un usuario del dominio (vienen generadas del script usado al principio):

s.chisholm:FallOutBoy1!

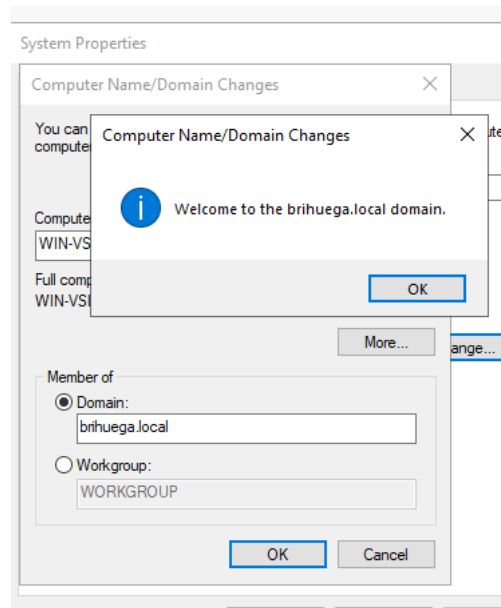


Ilustración 18. Anexión de SRV al dominio brihuega.local

Una vez hecho esto, se debe reiniciar el equipo. Al hacer el logon, ya aparecerá el dominio y se autentica con las credenciales del usuario del dominio. Una vez hecho, yendo a Server Manager – Local server, se puede ver que está incluido:

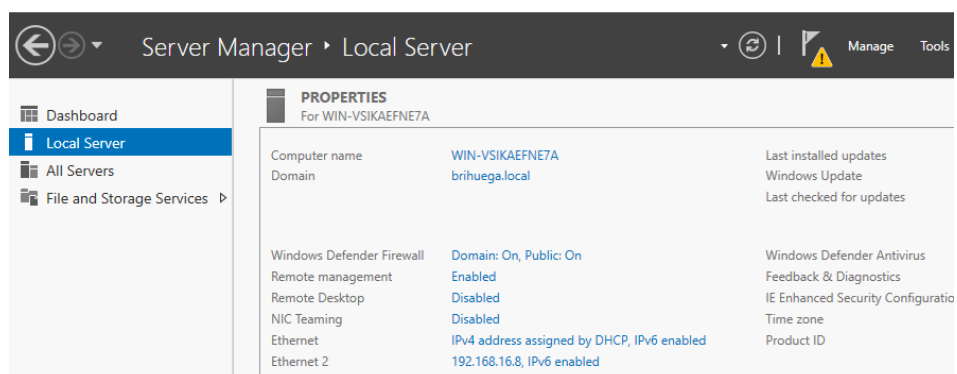


Ilustración 19. Anexión SRV al dominio brihuega.local

También se puede chequear en el DC que ya está incluido:

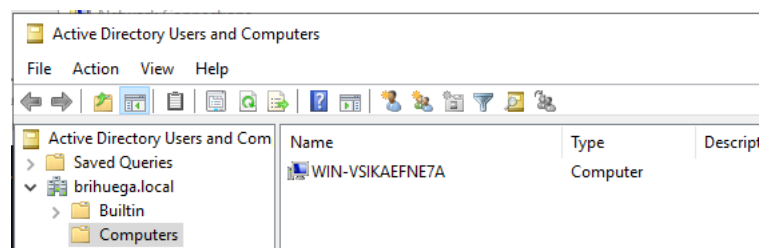


Ilustración 20. Comprobación en el DC la inclusión de SRV

## Configuraciones de seguridad

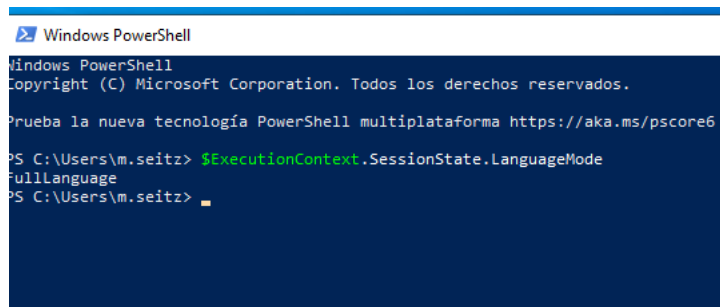
Se incluyen medidas de seguridad adicionales sobre las máquinas como AppLocker, CLM (Constrained Language Mode) o AMSI (Interfaz de examen antimalware).

A continuación, se explicará como instalar estas medidas en cada máquina. Otra opción es crear directivas (GPO) desde el DC, que se apliquen a las máquinas que están en el dominio.

### Configuración CLM (Constrained Language Mode)

Por defecto, se encuentra en “Full Language”. Para comprobarlo, se ejecuta el siguiente comando:

```
$ExecutionContext.SessionState.LanguageMode
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\m.seitz> $ExecutionContext.SessionState.LanguageMode
FullLanguage
PS C:\Users\m.seitz>
```

Ilustración 21. Full language por defecto

A continuación, se detallan los pasos para configurarlo como variable de entorno. Accediendo a panel de control -> sistema y seguridad-> Sistema-> Configuración avanzada del sistema -> Variables de entorno

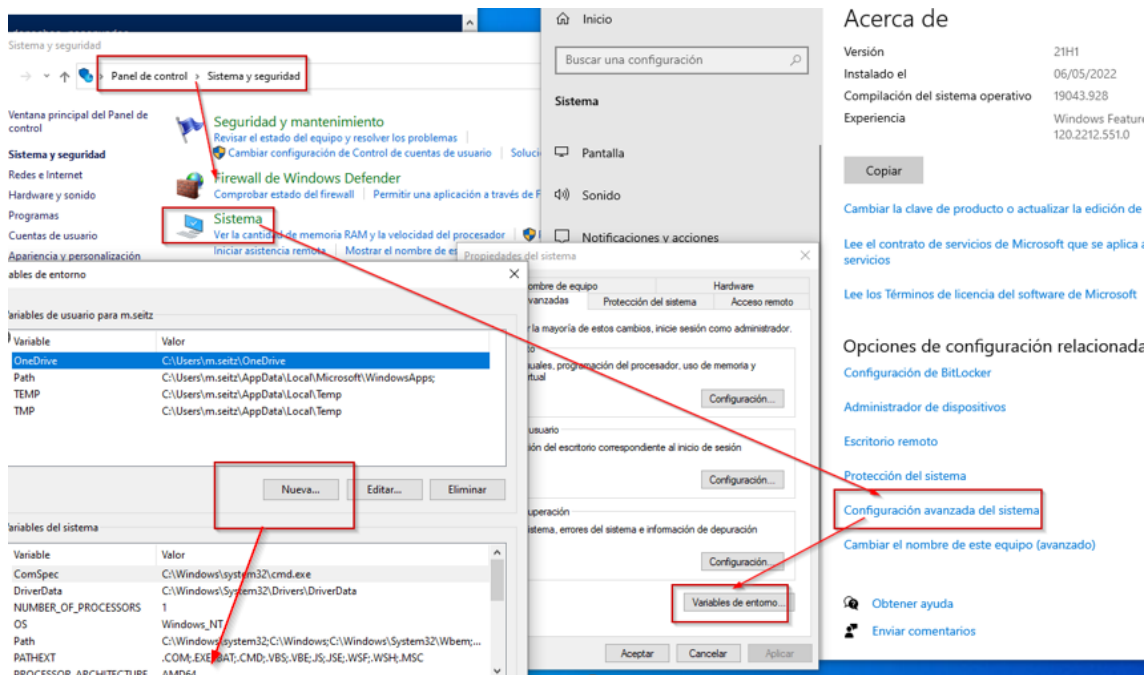


Ilustración 22. Configuración CLM como variable de entorno



A continuación, se añade una nueva:

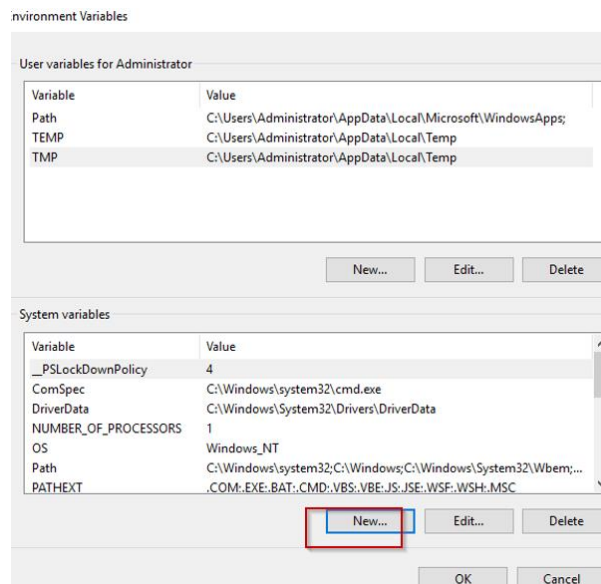


Ilustración 23. Adición CLM como variable de entorno

Y se añade lo siguiente:

- Nombre variable: \_\_PSLockDownPolicy
- Valor variable: 4

A continuación, reiniciando si se tuviera una consola de ps1, ya aparecerá configurado:

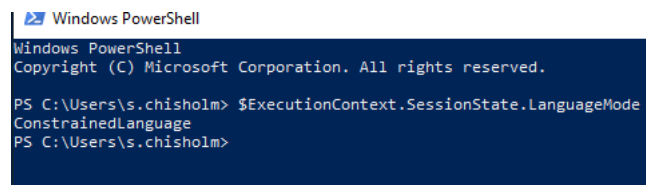


Ilustración 24. CLM configurado

Se comprueba con unos comandos:

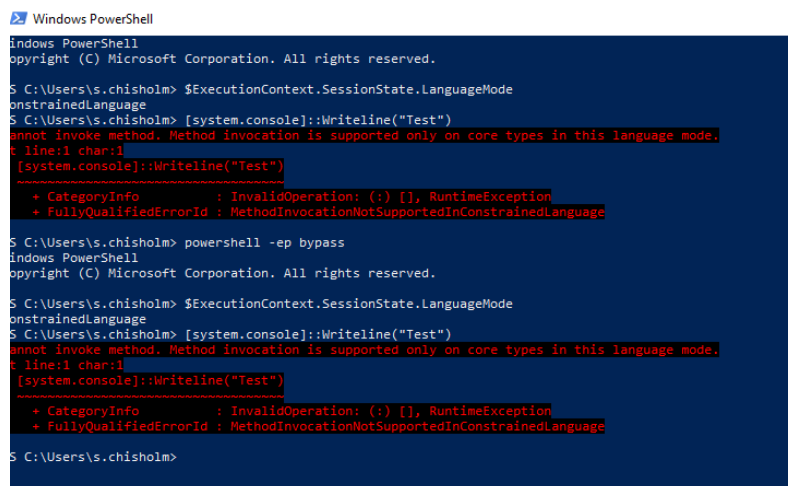


Ilustración 25. Testeo CLM

Otra opción es añadir como GPO o política. Desde una consola con permisos de administrador local se accede al registro y se crea una nueva:

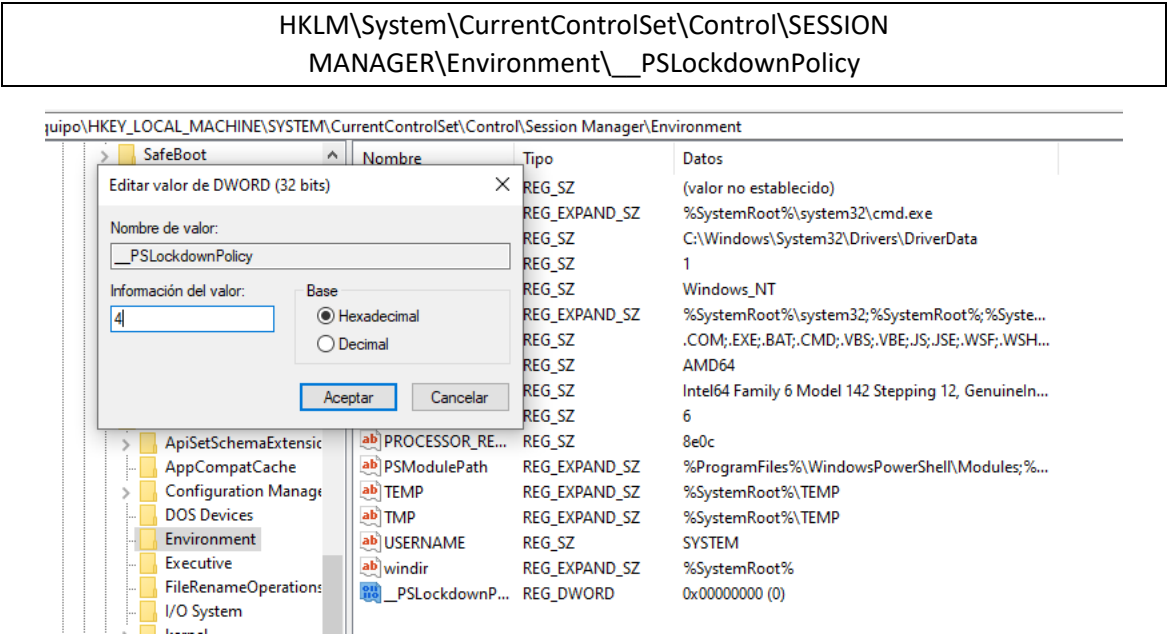


Ilustración 26. CLM mediante registro

Configuración AppLocker

Desde una consola con permisos de administrador, se accede al editor de directivas de grupo local gpedit.msc. Se accede a la ruta: Configuración del equipo -> Configuración de seguridad -> Directivas de control de aplicaciones -> Applocker y se despliega.

A continuación, se accede en reglas de scripts y ejecutables y se crean las reglas por defecto.

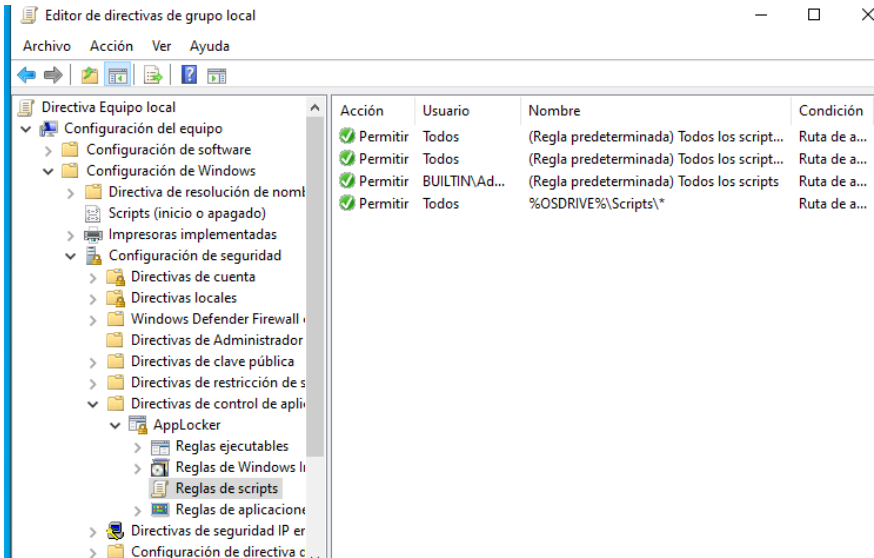


Ilustración 27. Configuración AppLocker

En este caso, se ha creado una regla adicional que permite la ejecución de scripts/ejecutables en la carpeta C:\Scripts

A continuación, sobre Applocker, se habilitan los checkbox para forzar a su ejecución:

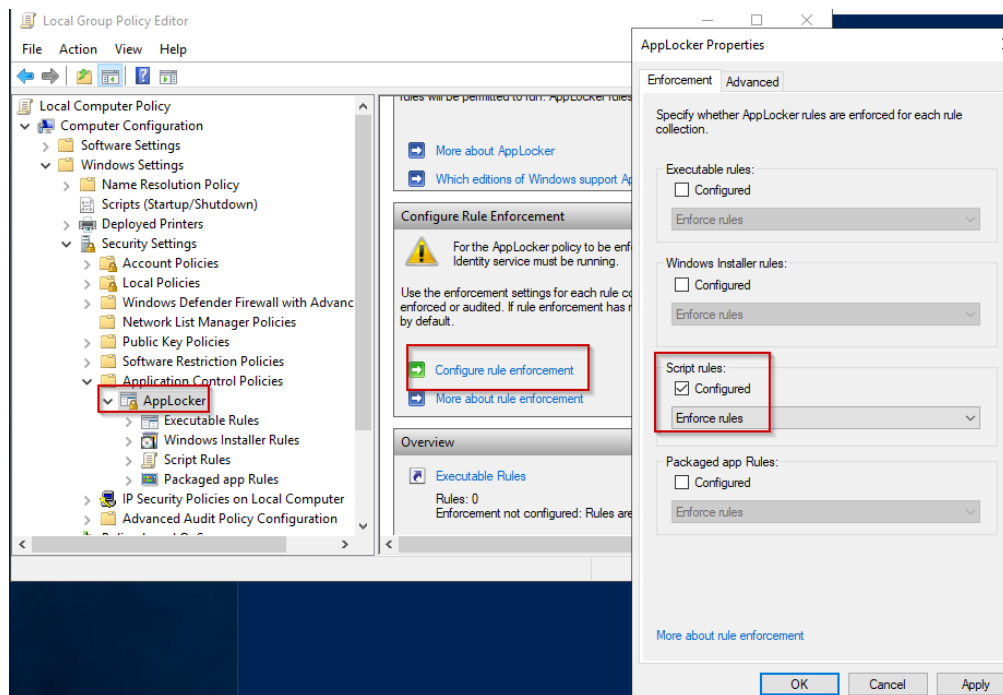


Ilustración 28. Configuración AppLocker

A continuación, se debe arrancar el servicio “Application Identity”. Para ello, desde una consola con permisos de administrador se debe ejecutar el siguiente comando:

```
sc config AppIDSvc start=auto
```

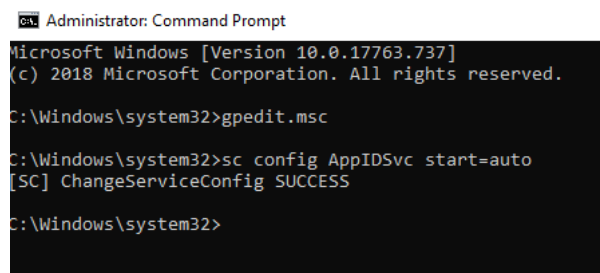


Ilustración 29. Arrancado el servicio Application identity

Esto va a hacer que se ejecute de manera automática también cuando se reinicie la máquina. Posteriormente, se puede acceder a “servicios” para ver qué efectivamente se encuentra en ejecución:

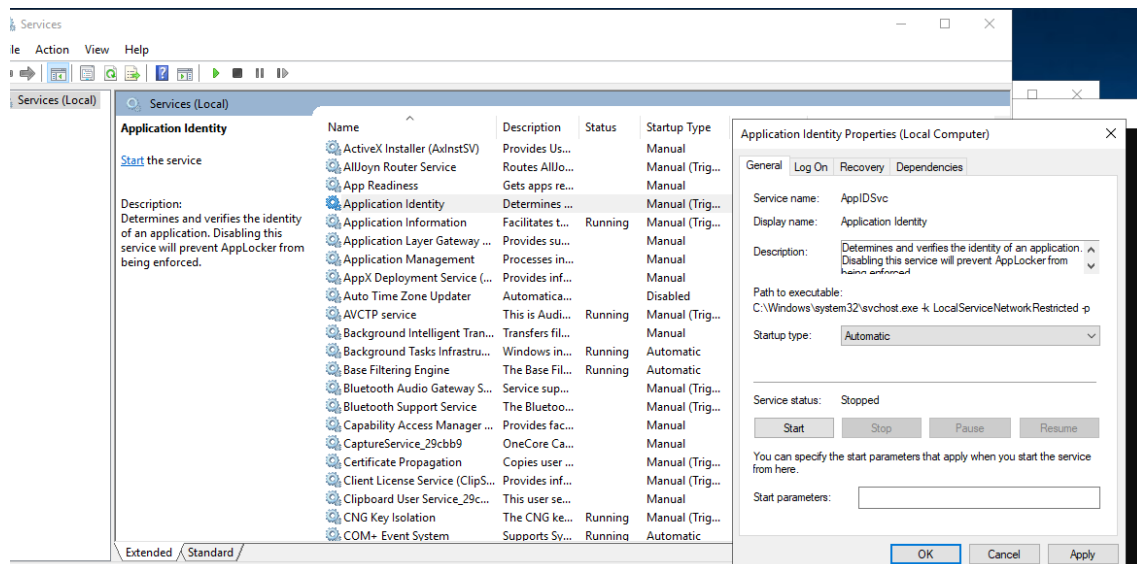


Ilustración 30. Comprobación servicio application identity

Finalmente, hay que reiniciar el equipo para que se apliquen las reglas de Applocker.

Por ejemplo, al ejecutar un script fuera de la carpeta permitido con un usuario que no es administrador, se bloquea su ejecución:

```
PS C:\Users\m.seitz\Downloads> ls

Directorio: C:\Users\m.seitz\Downloads

Mode                LastWriteTime         Length Name
----                -
-a----           01/06/2022   21:04             27 allowed.ps1

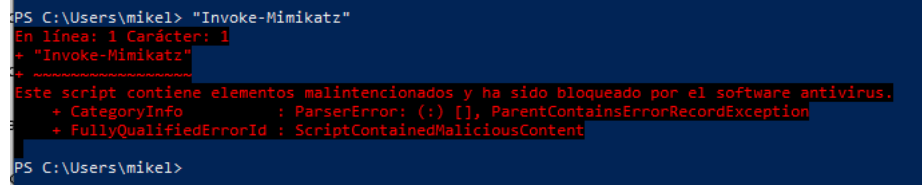
PS C:\Users\m.seitz\Downloads> .\allowed.ps1
.\allowed.ps1 : No se puede cargar el archivo C:\Users\m.seitz\Downloads\allowed.ps1 porque la ejecución de scripts
está deshabilitada en este sistema. Para obtener más información, consulta el tema about_Execution_Policies en
https://go.microsoft.com/fwlink/?LinkID=135170.
En línea: 1 Carácter: 1
+ .\allowed.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Ilustración 31. Bloqueo script por Applocker

Desde una consola con permisos de administración no se aplica las reglas de CLM ni Applocker (tal y como está con las reglas por defecto).

## Configuración AMSI

Por defecto viene habilitado. Para comprobarlo desde una consola de ps1 ejecutando “Invoke-Mimikatz”:



```
PS C:\Users\mikel> "Invoke-Mimikatz"
En línea: 1 Carácter: 1
+ ~~~~~
+ "Invoke-Mimikatz"
+ ~~~~~
Este script contiene elementos malintencionados y ha sido bloqueado por el software antivirus.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\mikel>
```

*Ilustración 32. Comprobación AMSI habilitado*

En el caso que no estuviera, se deben seguir los siguientes pasos (requieren permisos de administrador):

- Abrir el producto desde el menú **Inicio** de Windows.
- En la página principal, seleccionar, opciones.
- Seleccionar *Protección contra malware > Editar configuración*.
- Activar la Interfaz de análisis antimalware (AMSI).

## Generación tráfico

Se recomienda hacer un logon (sesión interactiva mediante PSSession o RDP) con un usuario administrador de dominio sobre la máquina SRV.

El resto de configuraciones que se verán en el laboratorio con el script inicial ADGenerator.ps1 ya estarían pre-cargadas.

## Referencias

<https://4sysops.com/archives/mitigating-powershell-risks-with-constrained-language-mode/#enabling-constrained-language-mode>

<https://www.techtarget.com/searchwindowsserver/tutorial/Increase-PowerShell-security-with-help-from-AppLocker>

<https://askme4tech.com/how-install-and-configure-applocker-improve-application-control-security>

<https://winbuzzer.com/2021/09/21/how-to-configure-applocker-in-windows-10-to-block-a-script-from-running-xcxwb/>

<https://www.hackingarticles.in/windows-applocker-policy-a-beginners-guide/>

<https://docs.microsoft.com/es-es/windows/win32/amsi/antimalware-scan-interface-portal>

<https://support.kaspersky.com/KIS/2021/en-us/186113.htm>

<https://techcommunity.microsoft.com/t5/exchange-team-blog/more-about-amsi-integration-with-exchange-server/ba-p/2572371>

<https://microsoft.github.io/CSS-Exchange/Admin/Test-AMSI/>

[https://help.f-secure.com/product.html?business/server-protection/latest/es-mx/task\\_ED11EEBB08DD4583AFA13EA59D3FC768-server-protection-latest-es-mx](https://help.f-secure.com/product.html?business/server-protection/latest/es-mx/task_ED11EEBB08DD4583AFA13EA59D3FC768-server-protection-latest-es-mx)