Como construir un diagrama

Como instalar y configurar Active Directory

Instalar y configurar Splunk

Instalar Windows 10 en virtual box

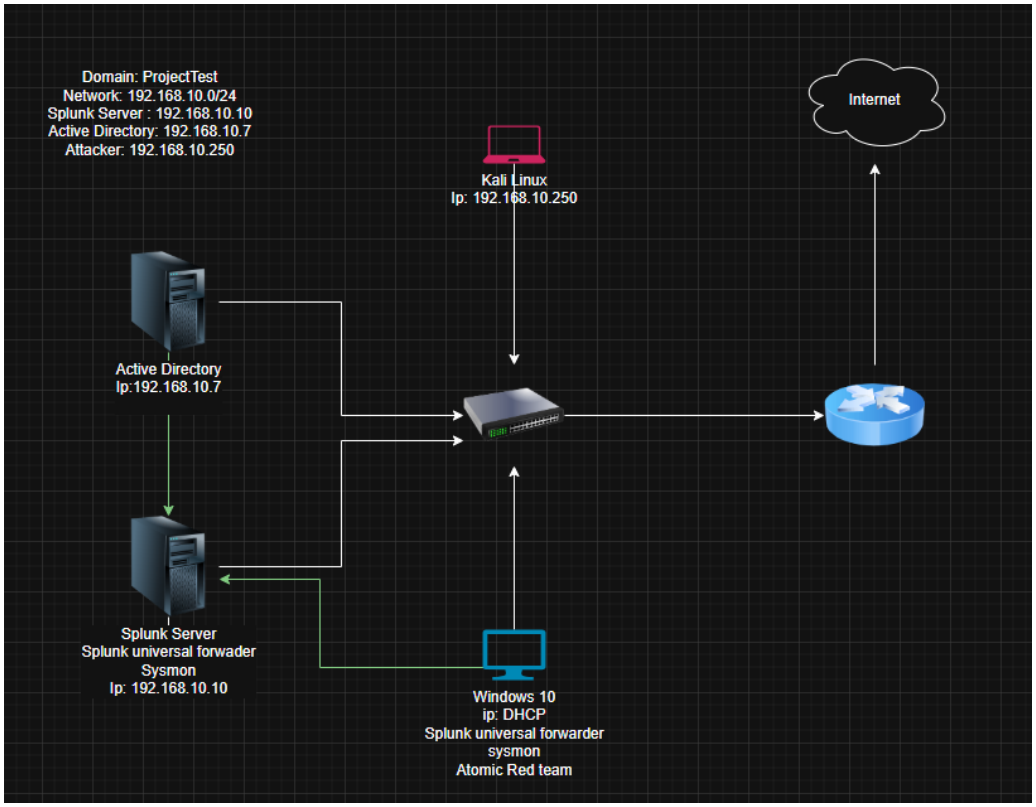
Instalar Windows server 2022 en virtual box

Correr pruebas con Atomic red team para generar telemetria

Realizar ataques de fuerza bruta para General telemetria

Como crear alerta , dashboard y reportes con splunk

1: Diagrama:



2- Active Directory:

Para usar AD se tiene que instalar el servicio active directory domain services

Y el servidor tiene que después ser promovido a domain controller, una vez se haga eso nos permitirá hacer autenticaciones usando kerberos y autorizaciones para el dominio.

AD DS: puedo tener objetos como: usuarios, computadores y grupos, y a su vez estos objetos tienen atributos:

Ejemplo: objeto usuario – bob

Atributos: primer nombre – bob, apellido -smith

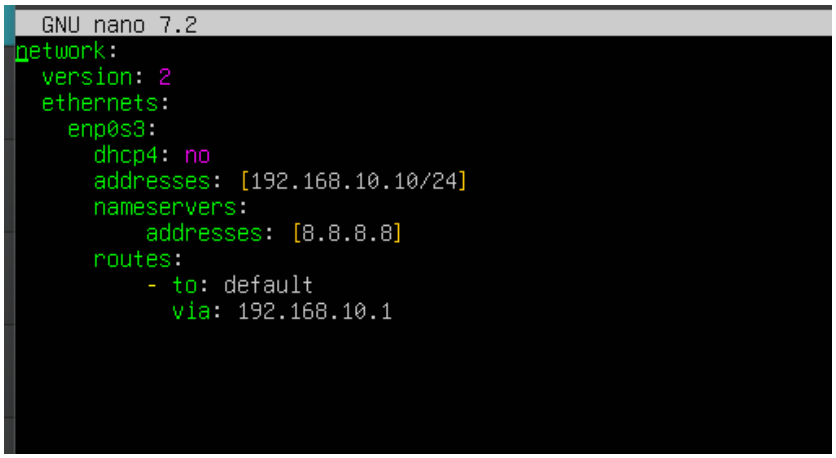
Para la creación de la imagen de Windows usaremos

https://www.microsoft.com/en-ca/software-download/windows10

instalar → luego saldrán opciones: si deseas actualizar el equipo o crear una imagen iso—> click en crear iso y siguiente y luego se procede a instalarla en el virtual box

modificaciones en el splunk server

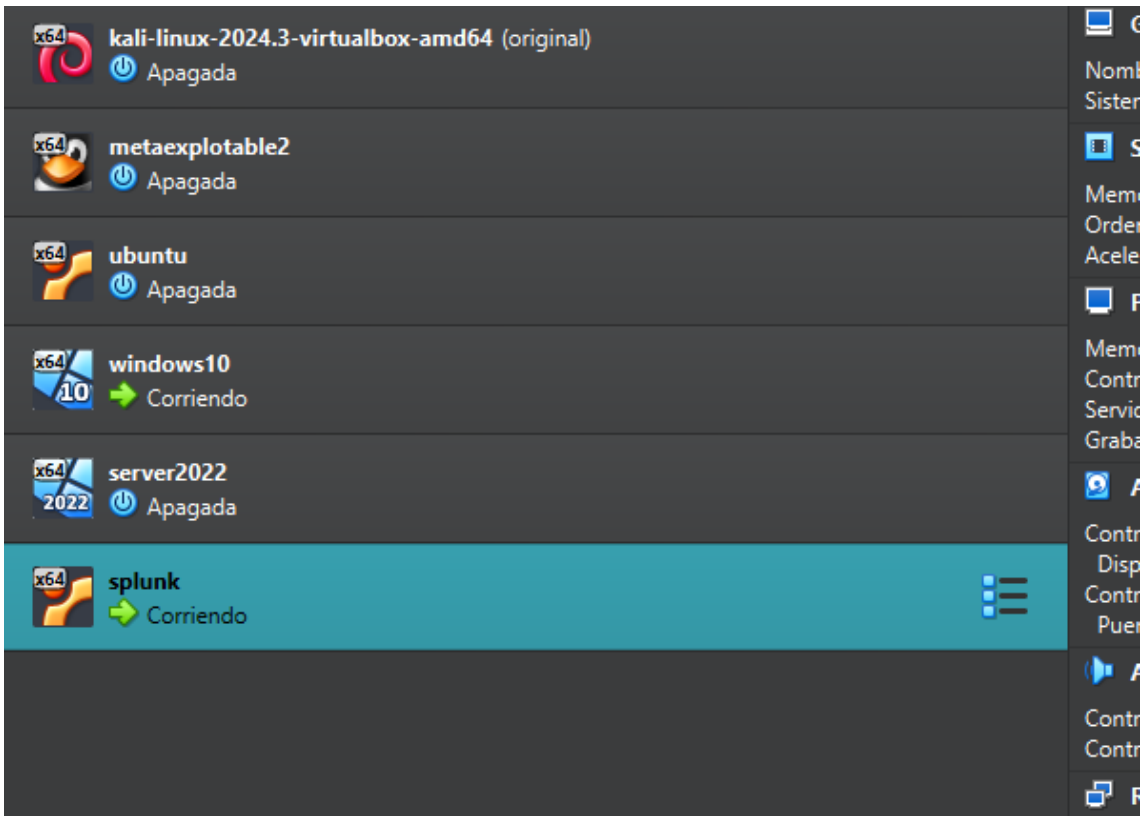

Para que tenga ip estática



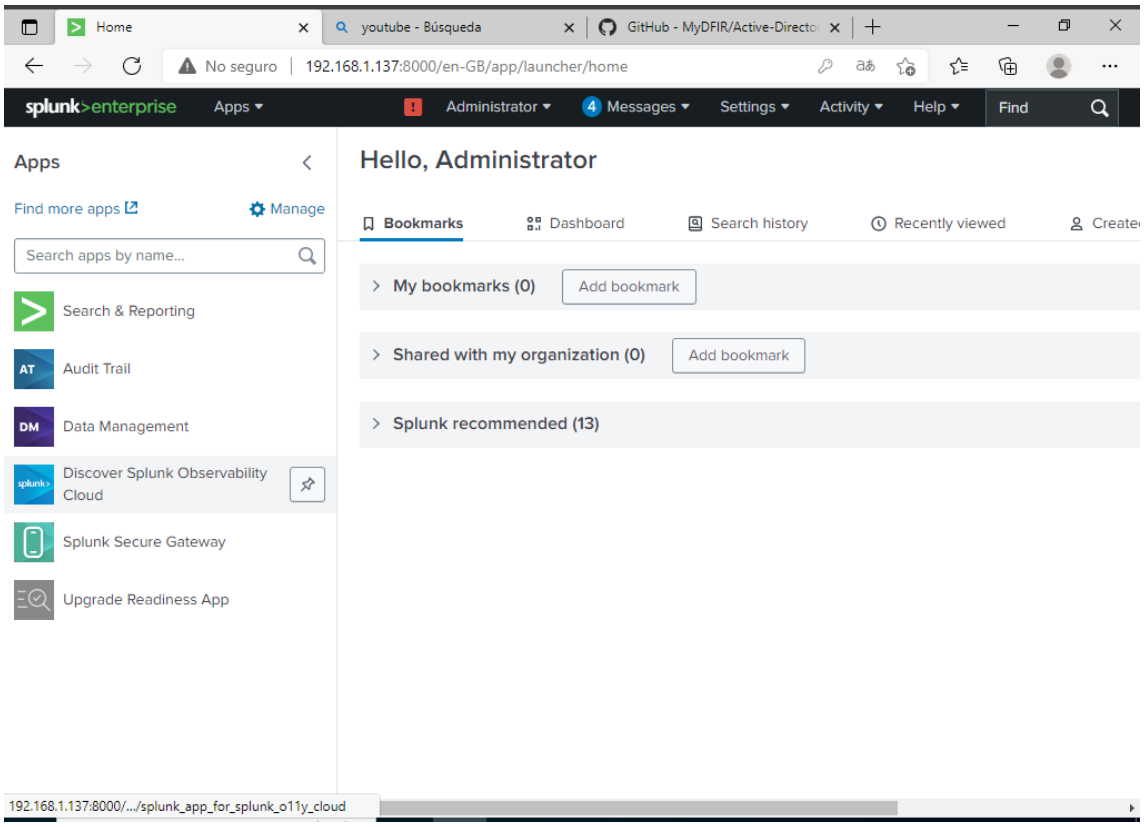
```
nameserver 127.0.0.53
options edns0 trust-ad
search .
```

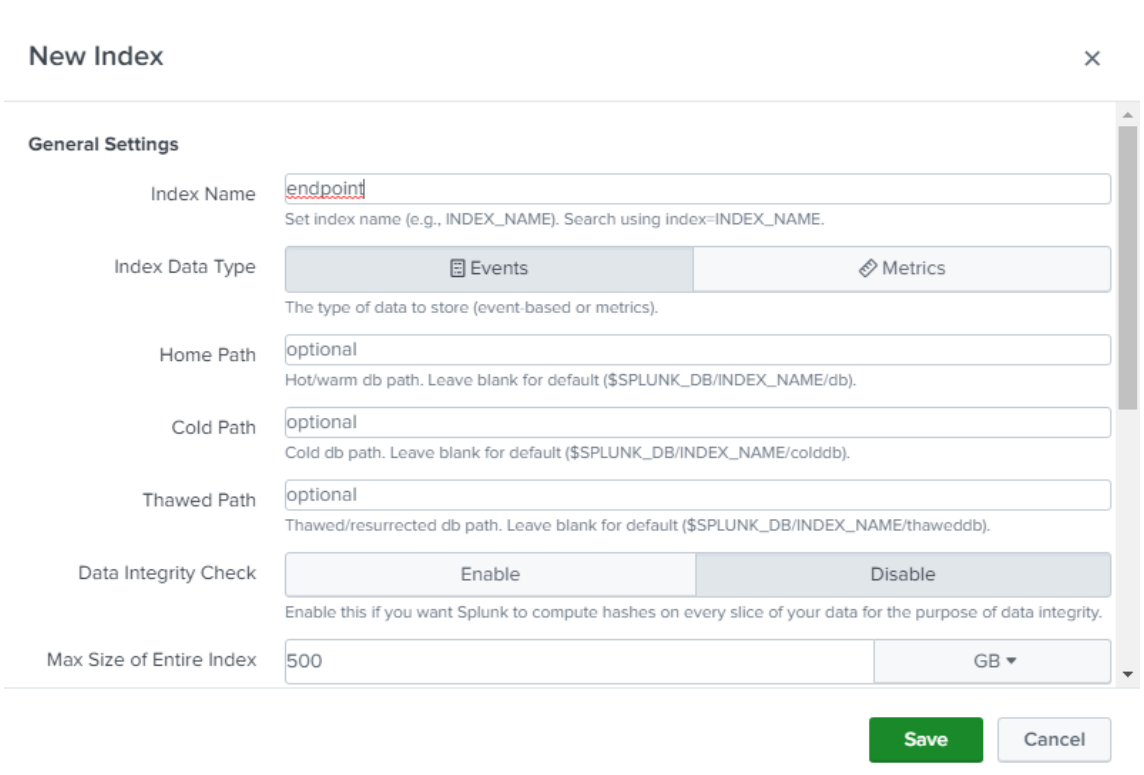
VirtualBox_VMs

```
johnny@splunk:/opt/splunk$ cd bin
johnny@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
johnny@splunk:/opt/splunk/bin$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:2e:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.137/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 85054sec preferred_lft 85054sec
    inet6 2a0c:5a81:6506:5d00:a00:27ff:fe5a:2efa/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe5a:2efa/64 scope link
       valid_lft forever preferred_lft forever
johnny@splunk:/opt/splunk/bin$
```




Windows -10


Home
youtube - Búsqueda
GitHub - MyDFIR/Active-Directo
No seguro
192.168.1.137:8000/en-GB/app/launcher/home
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Bookmarks
Dashboard
Search history
Recently viewed
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Splunk recommended (13)
192.168.1.137:8000/.../splunk_app_for_splunk_o11y_cloud


New Index
General Settings
Index Name
endpoint
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Index Data Type
Events
Metrics
The type of data to store (event-based or metrics).
Home Path
optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).
Cold Path
optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).
Thawed Path
optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).
Data Integrity Check
Enable
Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.
Max Size of Entire Index
500
GB
Save
Cancel

## Receive data

Configure this instance to receive data forwarded from other instances.

**Type**

Configure receiving

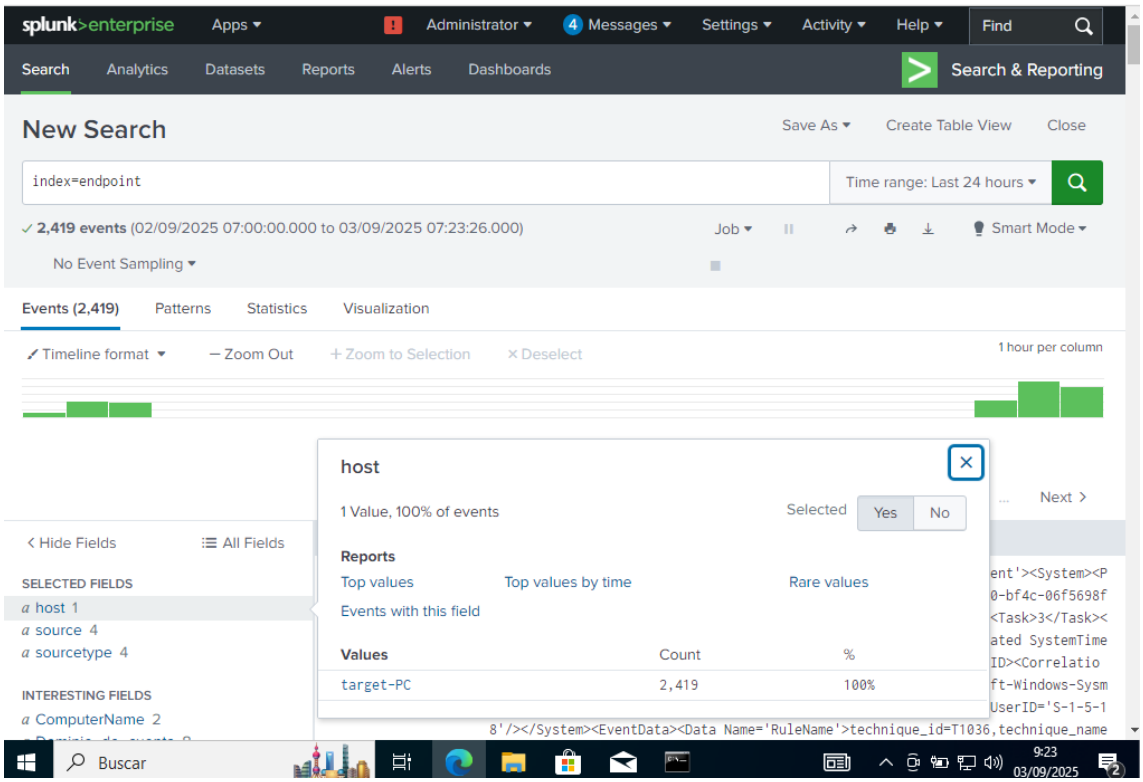
**Configure receiving**

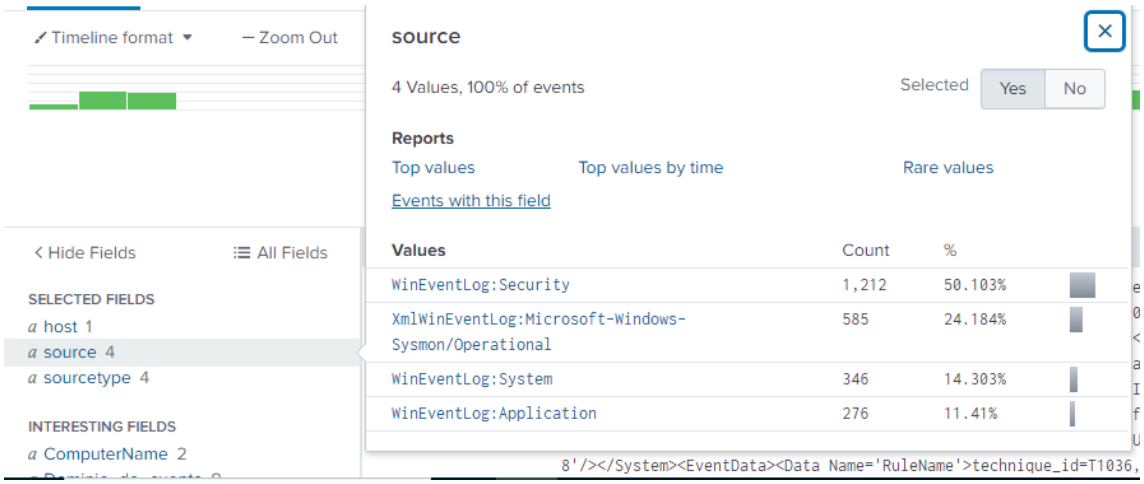
Set up this Splunk instance to receive data from forwarder(s).

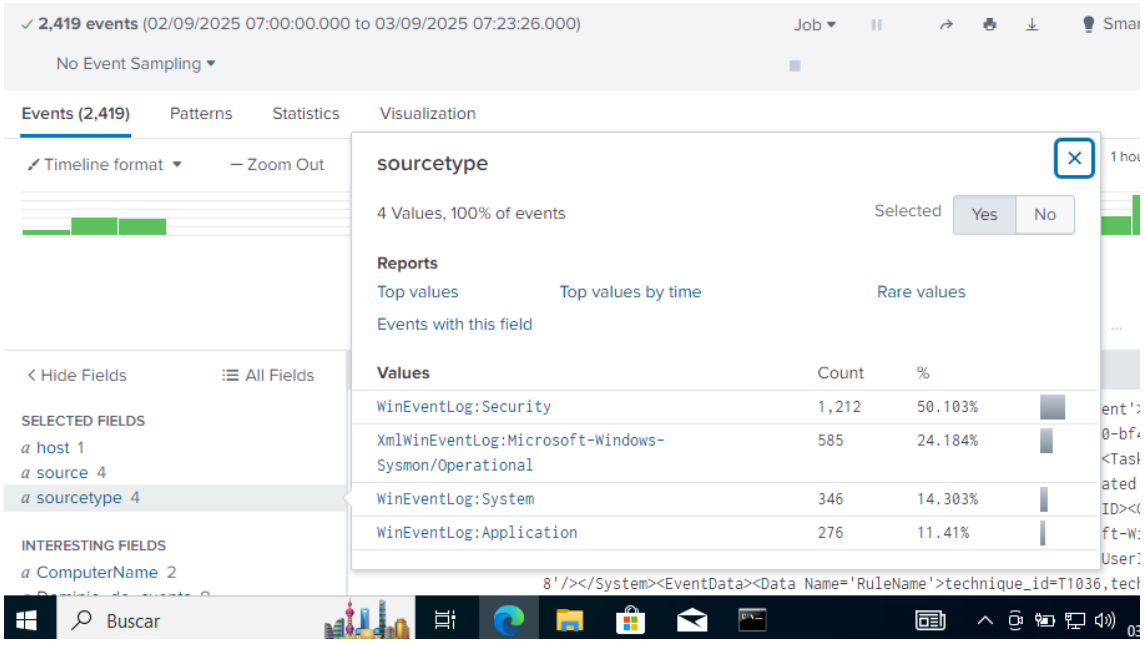
Listen on this port * 9997

For example, 9997 will receive data on TCP port 9997.

Cancel Save

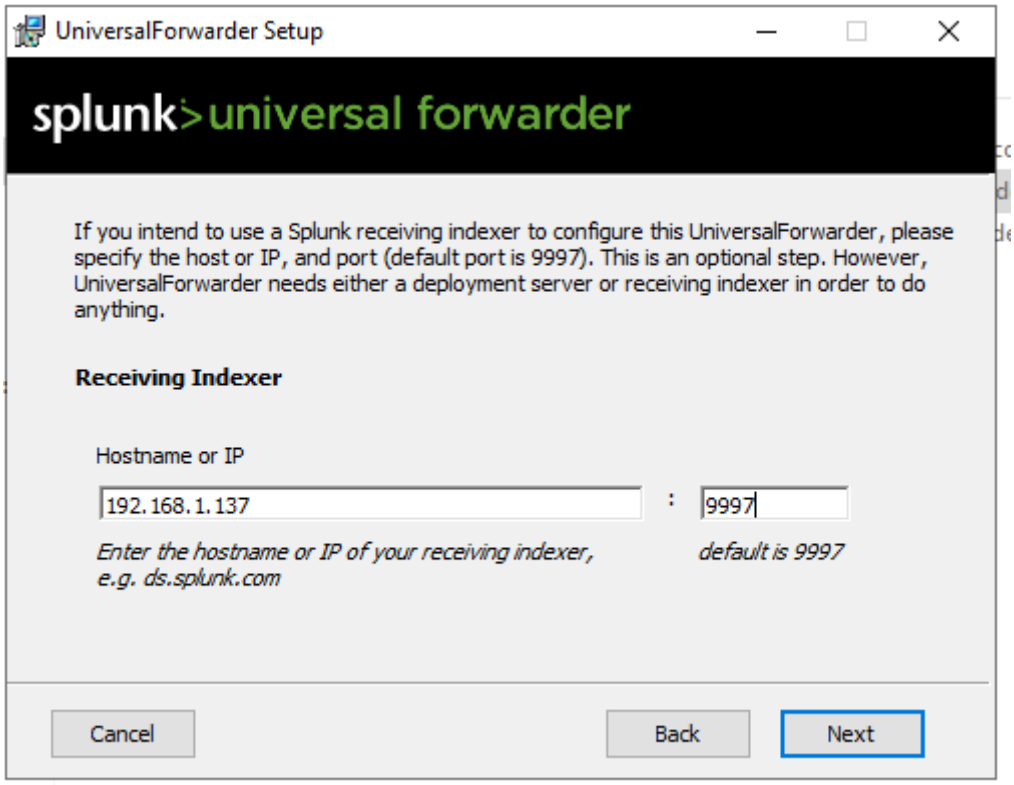





Servidor:

La ip pertenece al servidor splunk instalado




Descargamos sysmon:

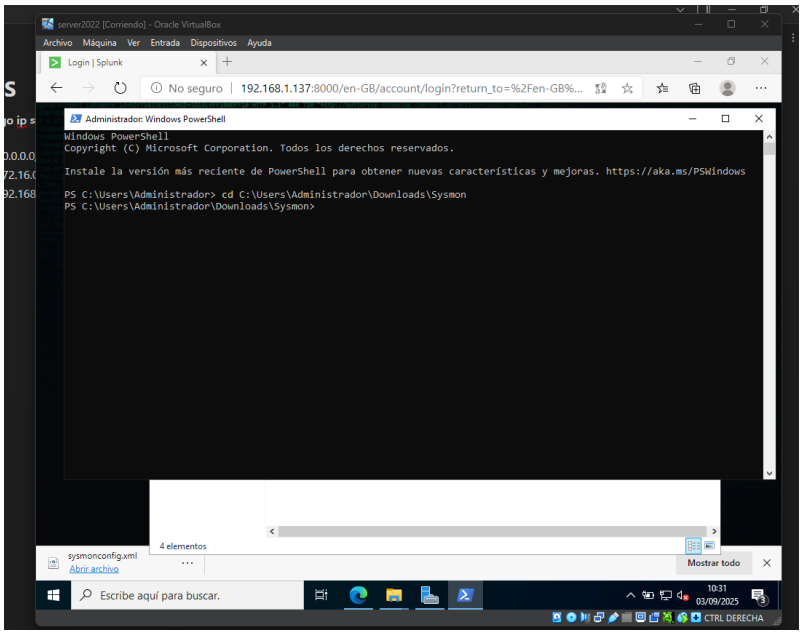
https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon

también el archivo de configuración sysmon olaf : https://github.com/olafhartong/sysmon-modular pero usamos el archivo:

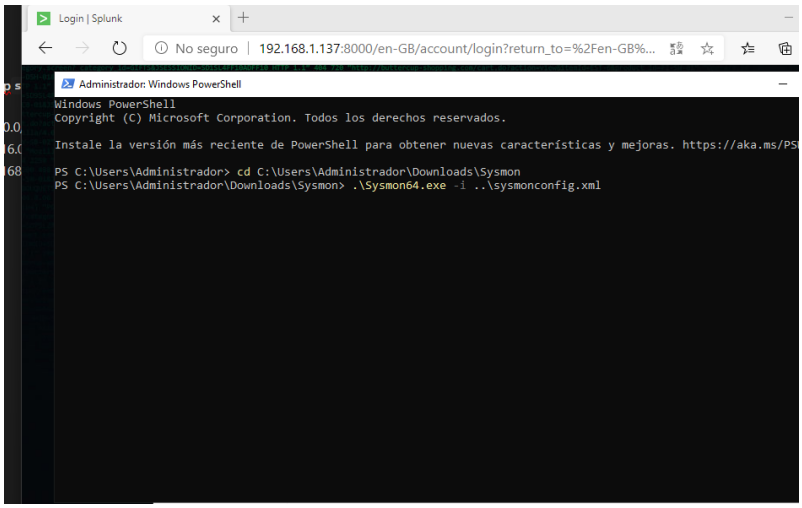
https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml

clic en raw y guardamos el archivo

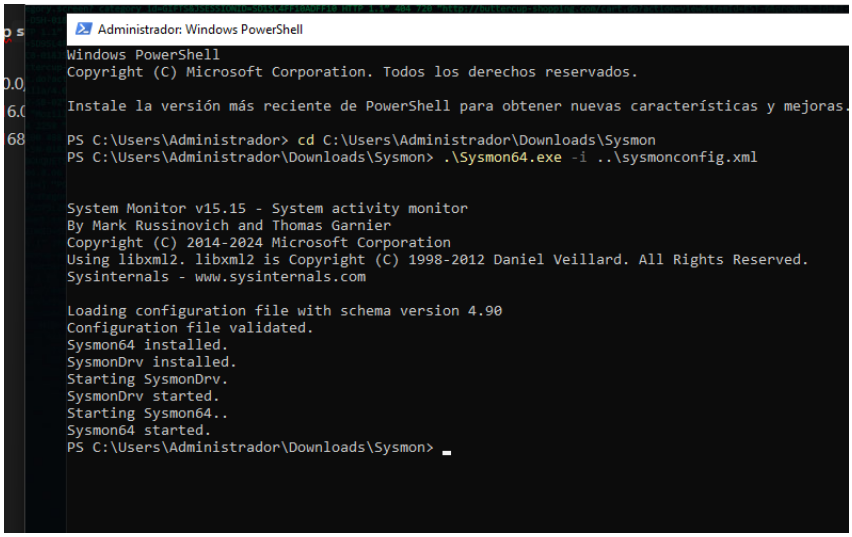
una vez descomprimo el archivo de sysmon , copiamos la ruta y vamos a PowerShell como administrador




Vamos a la siguiente ruta:




E instalamos sysmos



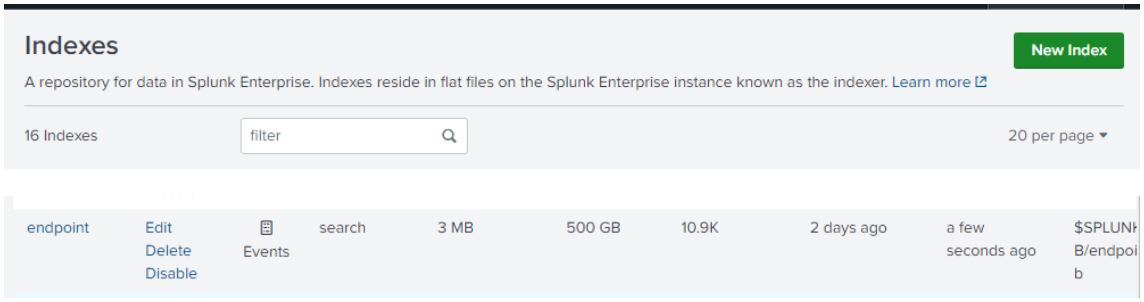
Configuraremos un archivo inputs.conf ( c:\program Files\splunkUniversalForwader\etc\system\default) que es la instrucción de splunk forwarder indicándole a donde queremos que envíe los datos ,métricas y demás estos datos se envían nuestro splunk server, haremos una copia en la carpeta ( c:\program Files\splunkUniversalForwader\etc\system\local), para evitar perder el original, y NO EDITARLO el archivo a editar lo editaremos así:

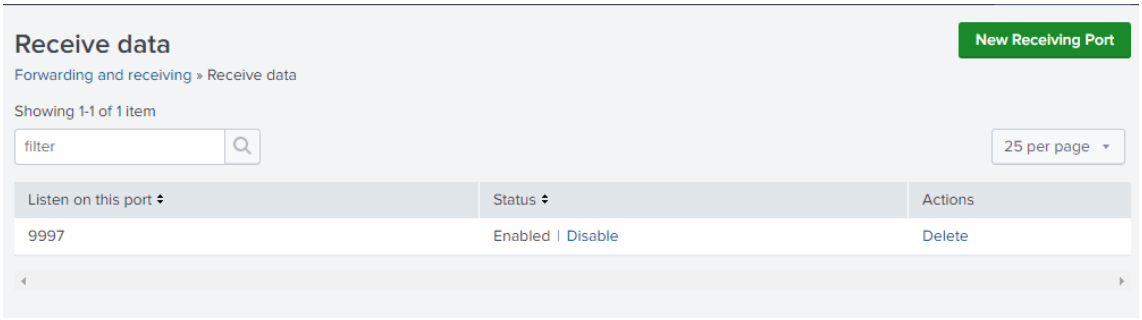
Lo que esto hace es decirle al splunk forwader que envíe datos relacionados a: aplicaciones, seguridad, sistema y sysmon al splunk server

```
[WinEventLog://Application]
index = endpoint
disabled = false
[WinEventLog://Security]
index = endpoint
disabled = false
[WinEventLog://System]
index = endpoint
disabled = false
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

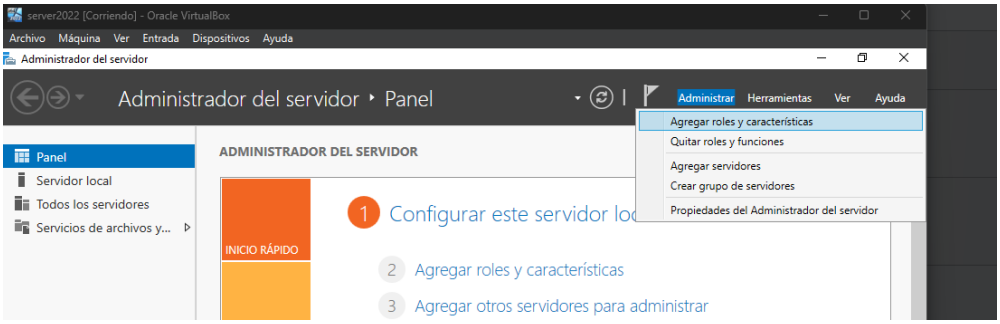
Una vez guardado a la copia reiniciamos el servicio de splunk forwader

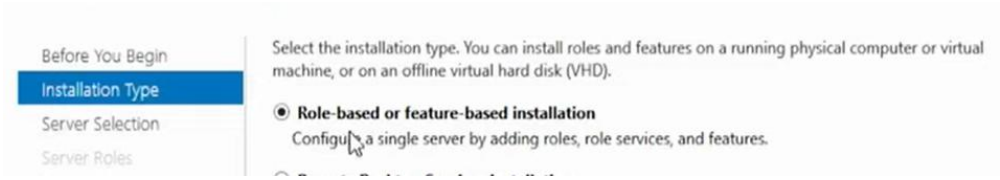
Y luego terminamos la configuración en splunk: agregamos el indexes que es endpoint y el puerto:

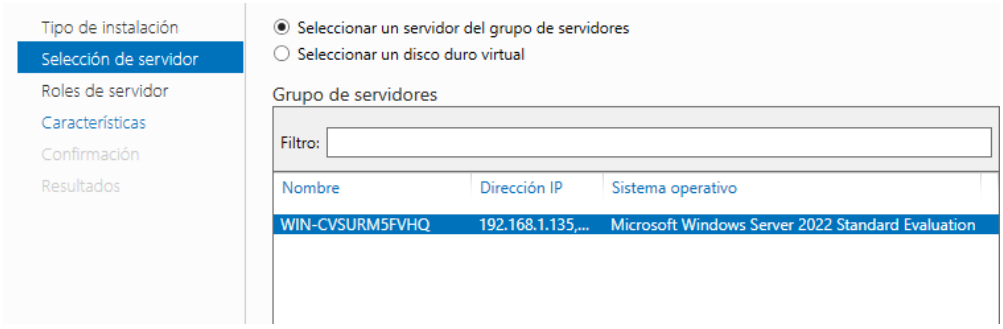


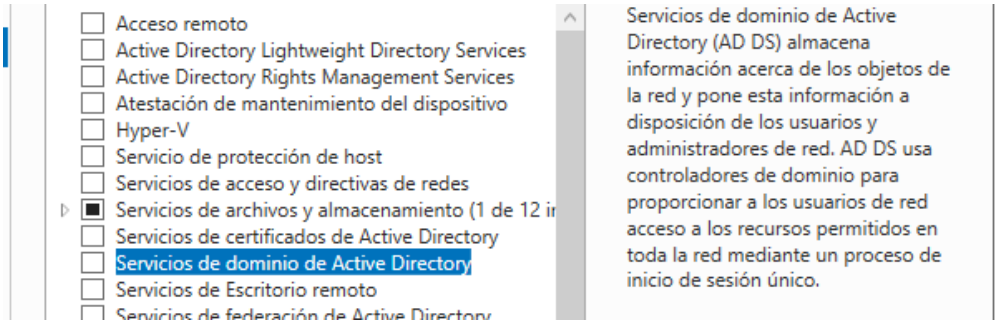


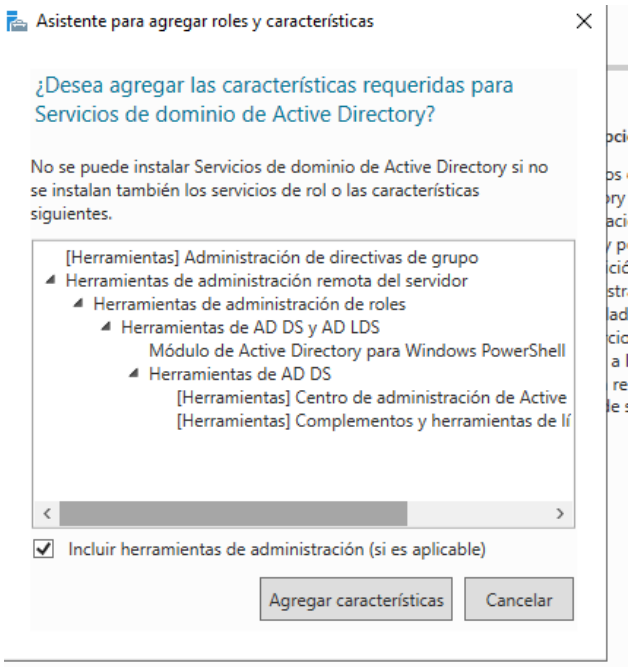

Ahora haremos el servidor un domain controller

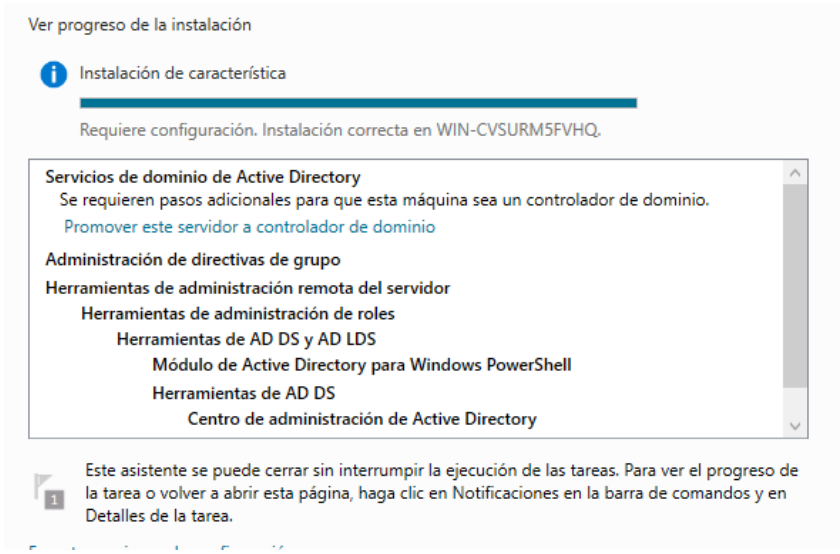


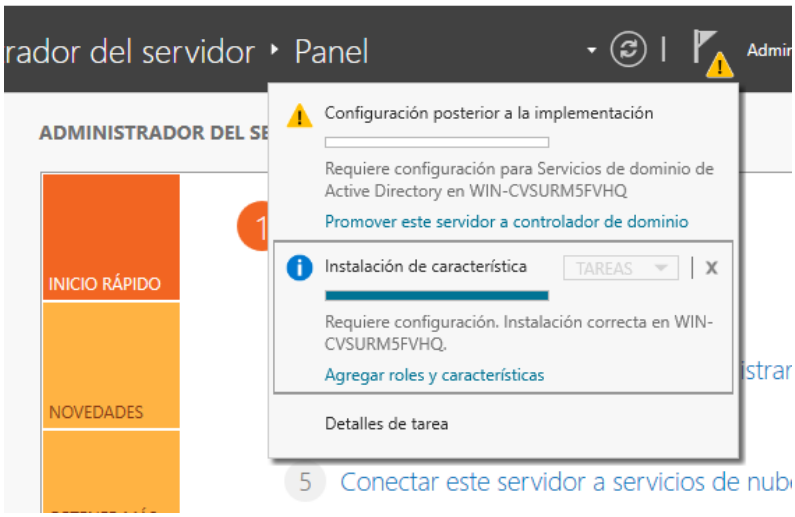



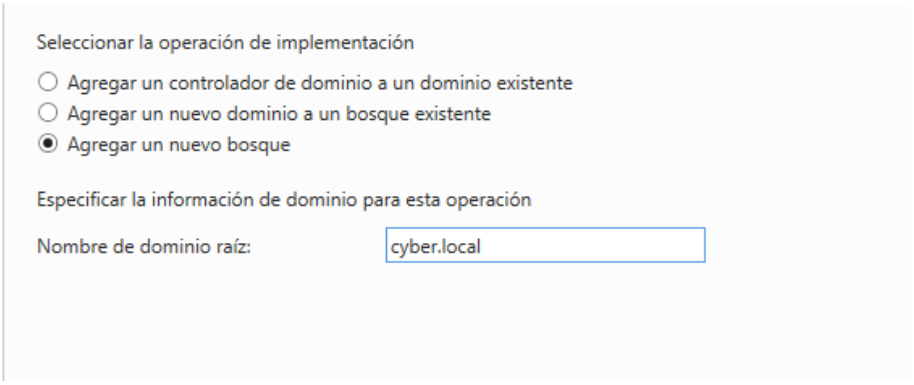


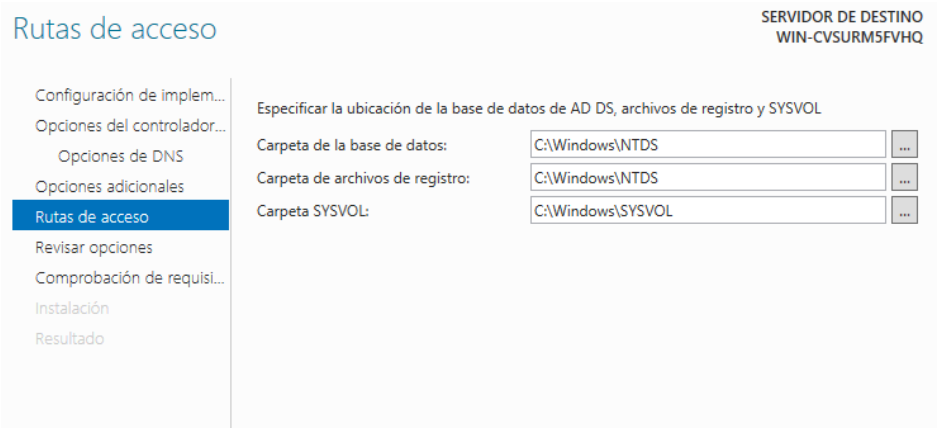

Clic en el triángulo de advertencia y seleccionar promover este servidor a controlador de dominio




Será el top level nivel

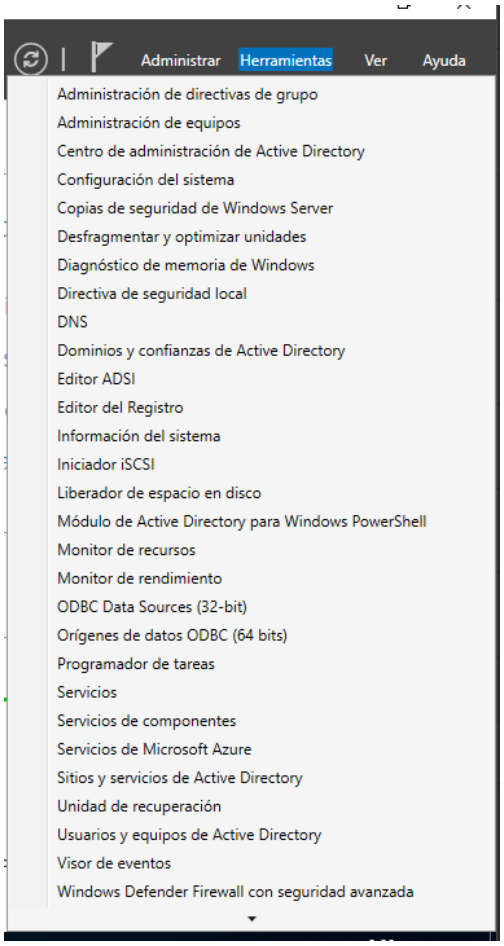


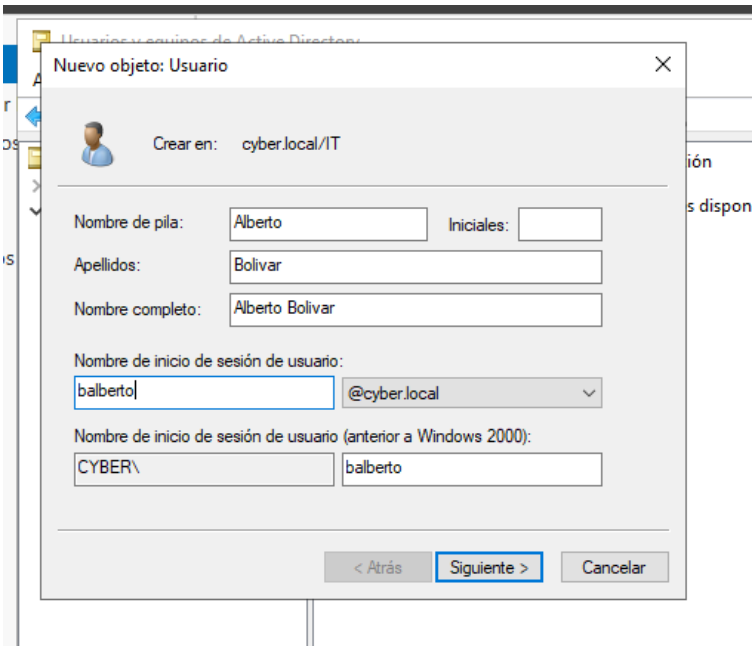

Acá se almacena toda la información del servidor, y este es el objetivo de los atacantes, ya que tiene hashes y demás




Una vez finalizado se reiniciará y ya habremos promovido el servidor a controlador de dominios e instalado AD

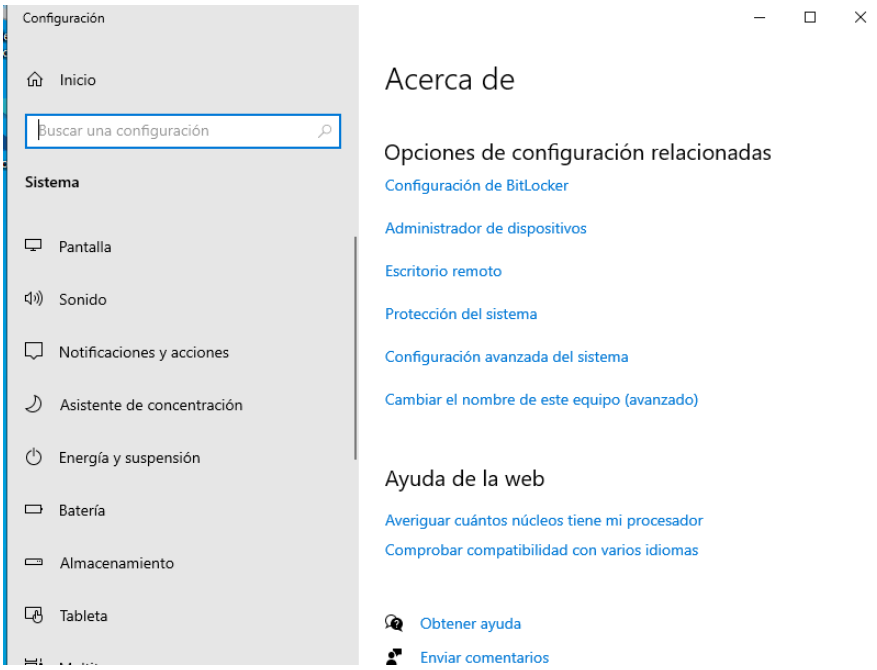

Usuarios y equipos de active directory



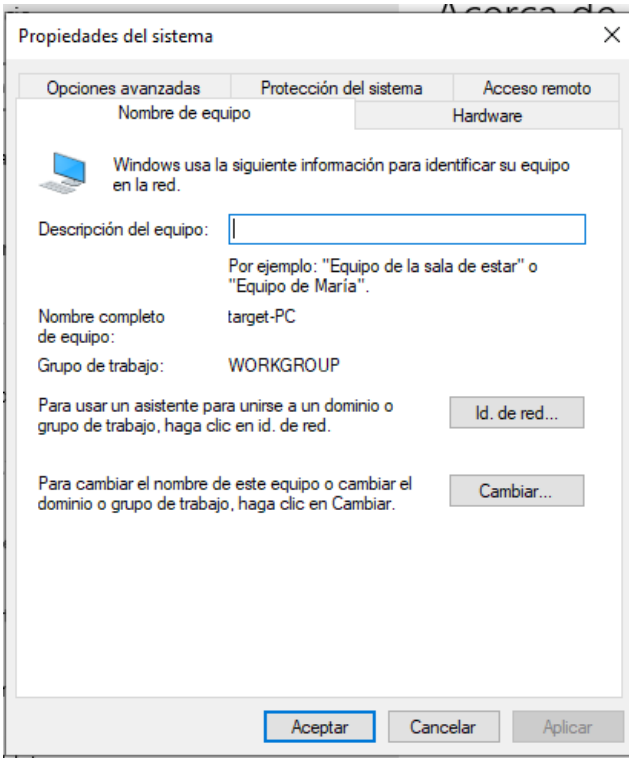



Ahora necesitamos unir nuestro pc normal al controlar de dominio del servidor

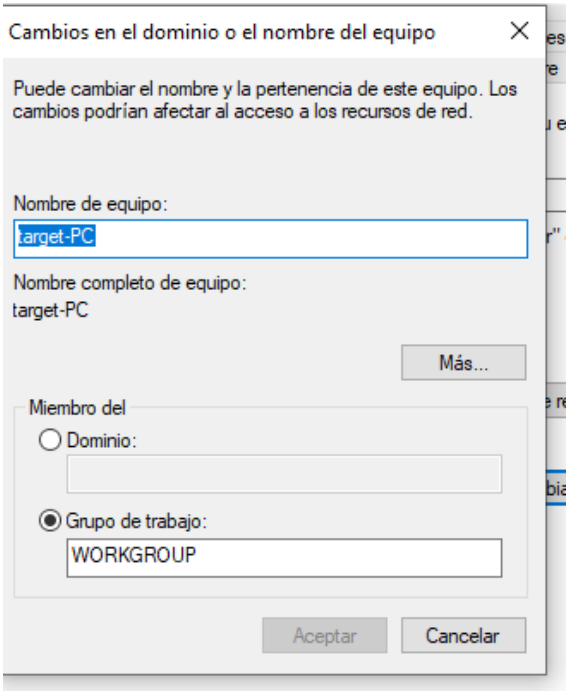
Barra de búsqueda: pc-→ propiedades-→

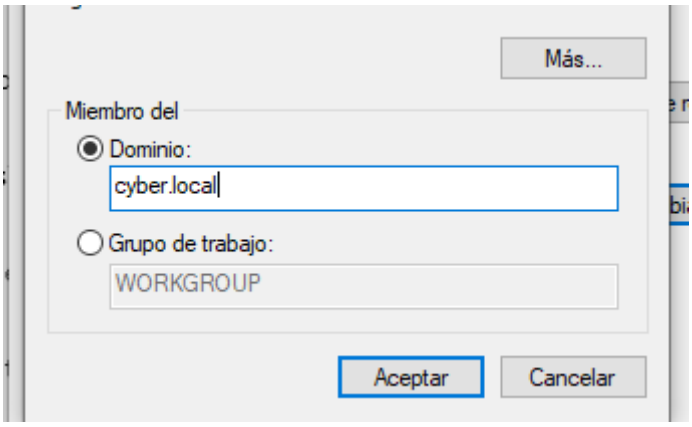



Configuración avanzada del sistema→ nombre equipo

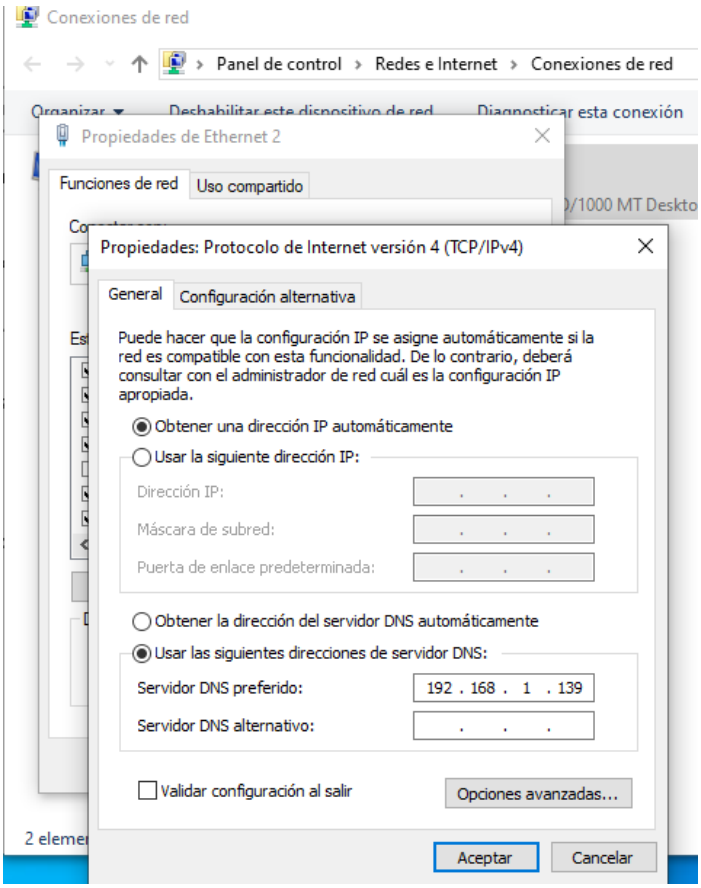


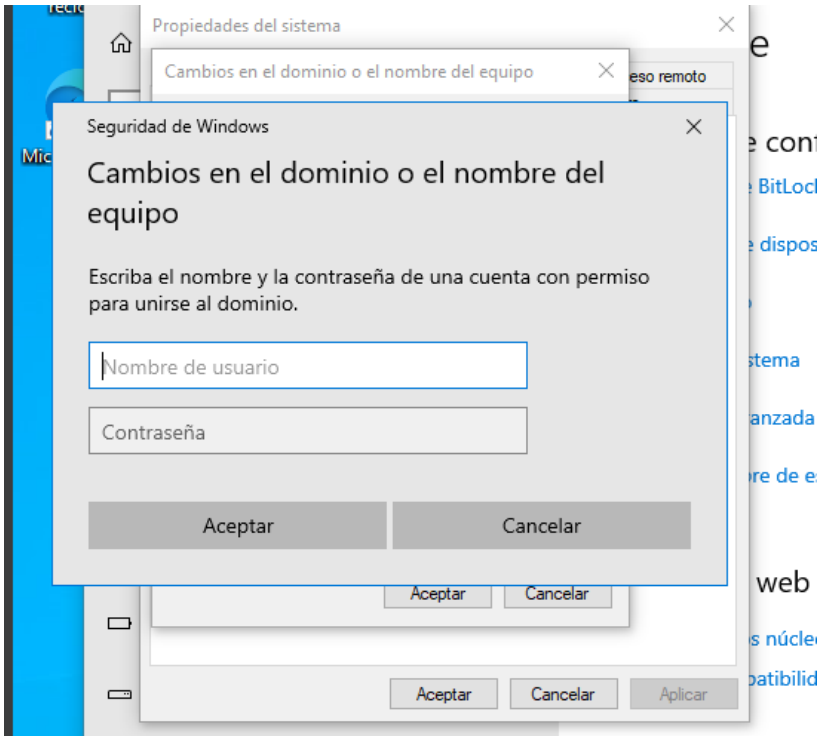

Cambiar→miembro del: y escribimos el nombre del dominio



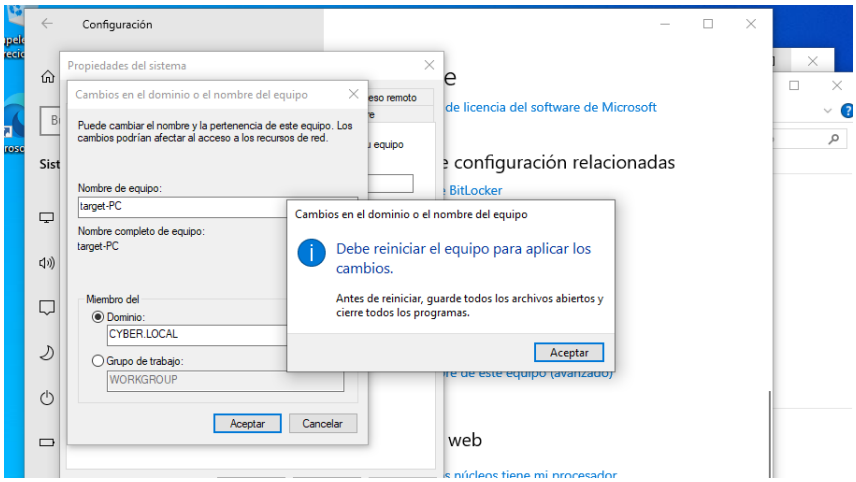



Al intentar agregarlo da un error ya que el pc no podría resolver el nombre de dominio dns, entonces tendríamos que configurarlo manualmente agregando el del servidor



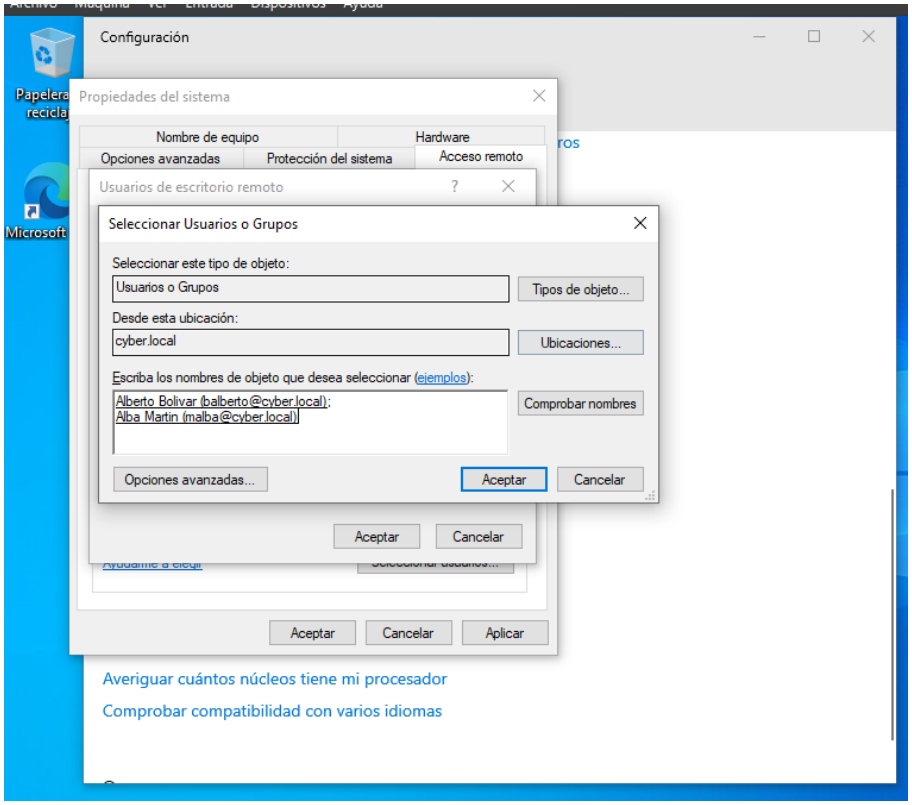



Usaremos la cuenta del administrador del servidor




Una vez reiniciado podemos iniciar sesión con uno de los usuarios creados

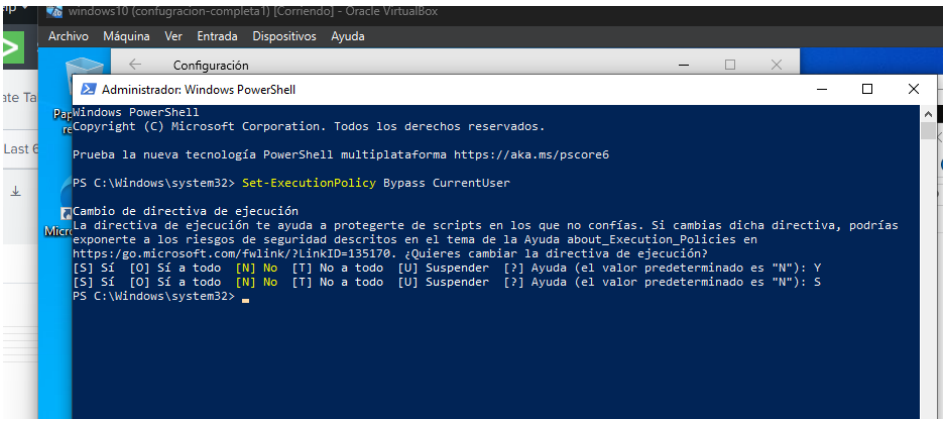

Una vez hecho todo esto procederemos a iniciar sesión con nuestro administrador en el target pc y habilitaremos el rdp para que los usuarios puedan acceder



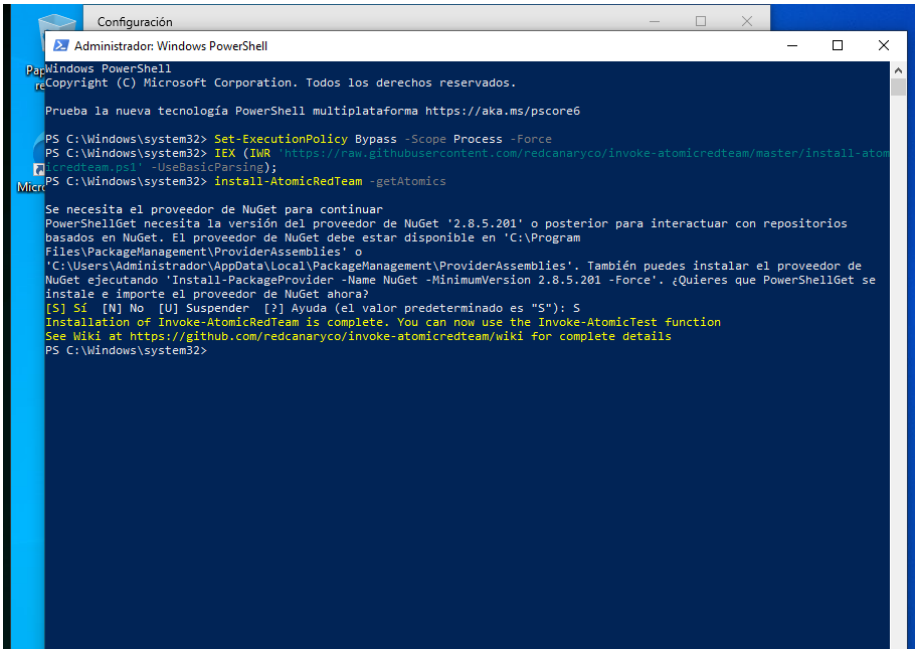

Ya con todo instalado y seteado, se puede hacer diferentes cosas para generar telemetría, como fuerzas brutas, ataques de phishing y demás.

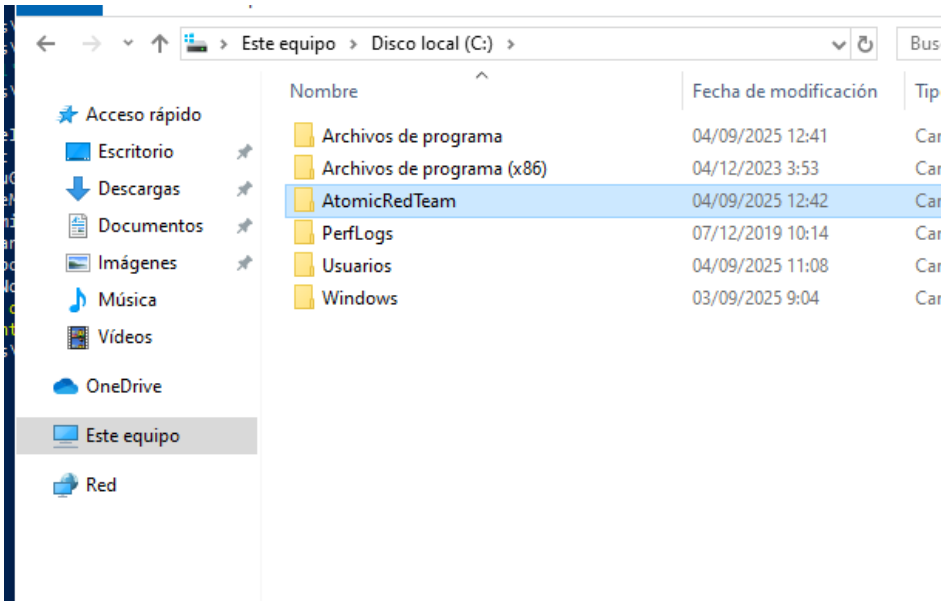
Instalar atomic red team

Iniciar sesión como administrador en el pc, y además arracar powershell como administrador

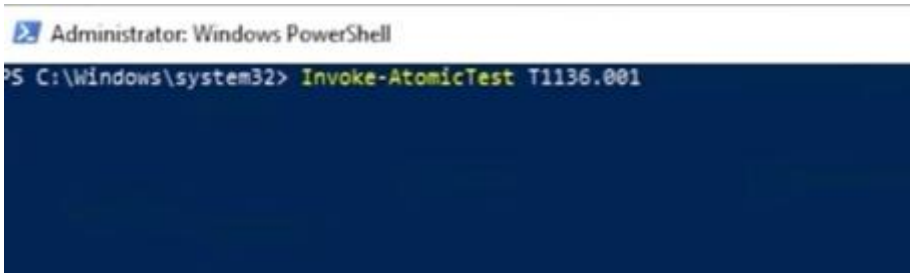



Hay que excluir la carpeta disco c: en el antivirus de Windows defender






La manera de invocar atomic red team desde el target pc como administrador desde PowerShell como administrador




Y de esa manera verificar la telemetría