

Como construir un diagrama

Como instalar y configurar Active Directory

Instalar y configurar Splunk

Instalar Windows 10 en virtual box

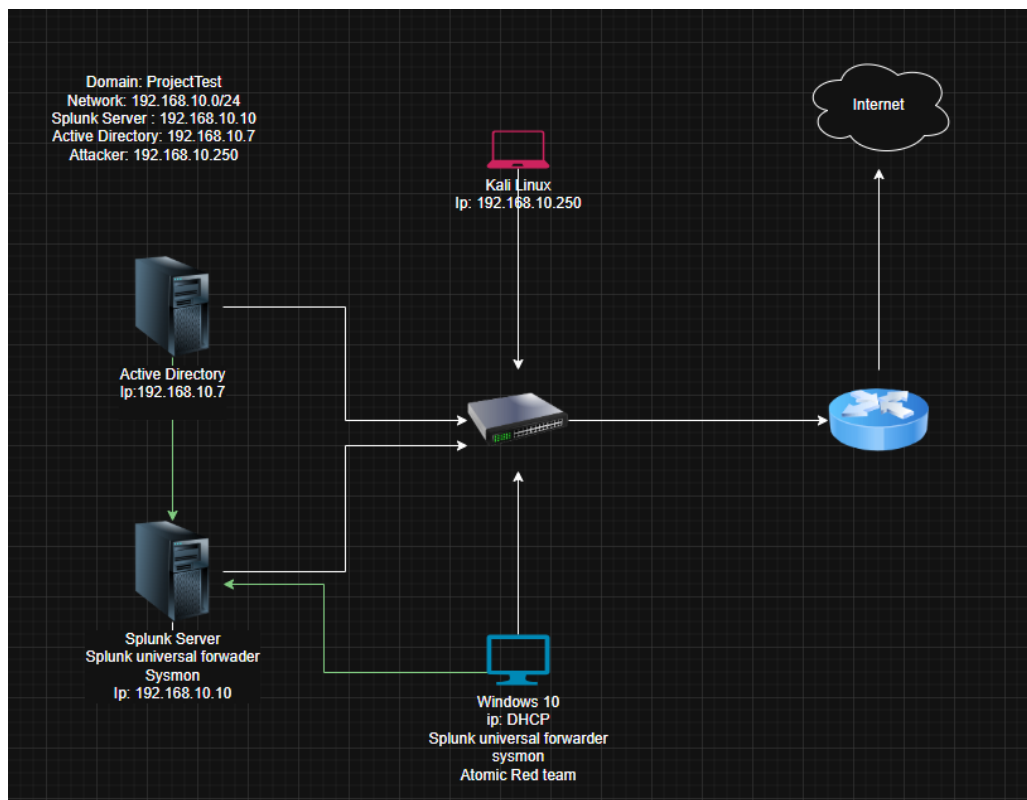
Instalar Windows server 2022 en virtual box

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

```
valid_ifit forever preferred_ifit forever
johnny@splunk:~$ sudo nano /etc/netplan/50-cloud-init.yaml _
```

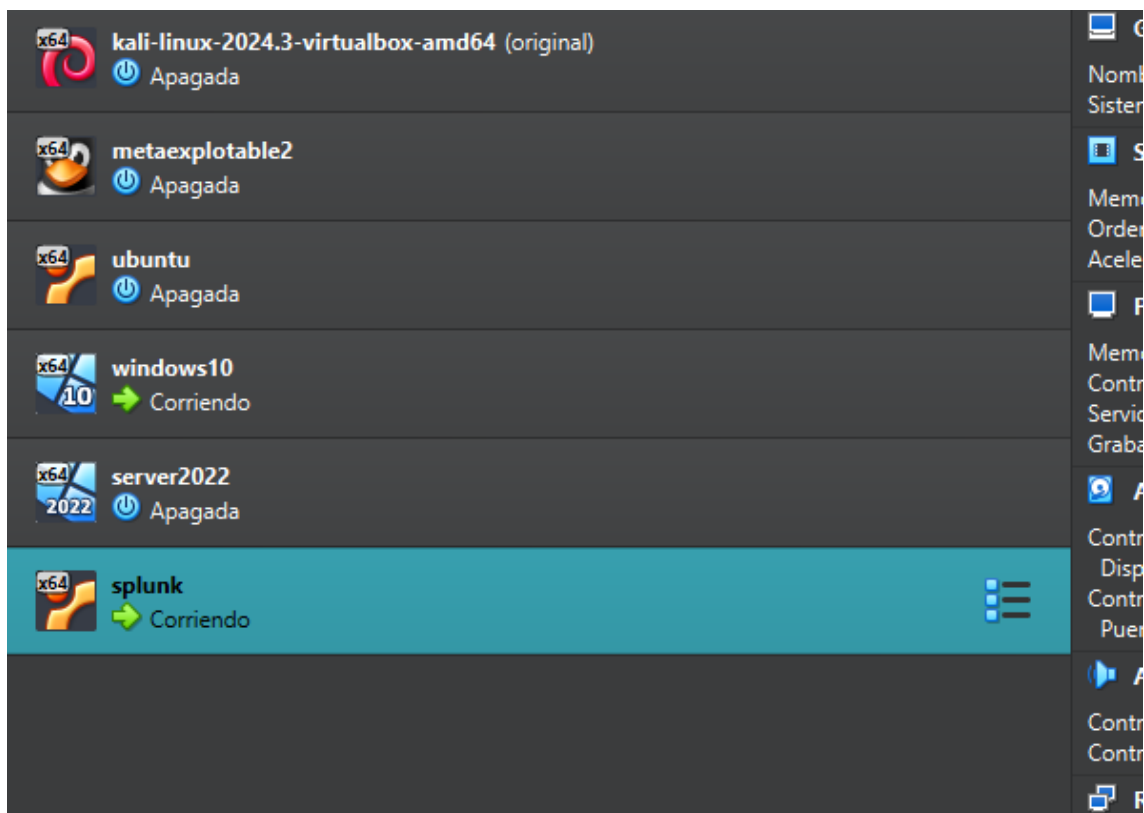
Para que tenga ip estática

```
GNU nano 7.2
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
        addresses: [8.8.8.8]
      routes:
        - to: default
          via: 192.168.10.1
```

```
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

AT Audit Trail

DM Data Management

Discover Splunk Observability Cloud

Splunk Secure Gateway

Upgrade Readiness App

Hello, Administrator

Bookmarks

Dashboard

Search history

Recently viewed

Create

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 | <input type="text" value="endpoint"/> |
| | Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME. |
| Index Data Type | <div><div>Events</div><div>Metrics</div></div> |
| | The type of data to store (event-based or metrics). |
| Home Path | <input type="text" value="optional"/> |
| | Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db). |
| Cold Path | <input type="text" value="optional"/> |
| | Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb). |
| Thawed Path | <input type="text" value="optional"/> |
| | Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb). |
| Data Integrity Check | <div><div>Enable</div><div>Disable</div></div> |
| | 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 | <div><input type="text" value="500"/><div>GB</div></div> |

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

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search' and shows a search for 'index=endpoint' with a time range of 'Last 24 hours'. It indicates that 2,419 events were found. Below the search results, there are tabs for 'Events (2,419)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is active, showing a timeline view. A modal window titled 'host' is open, displaying a report for the 'host' field. The report shows 'target-PC' as the top value with a count of 2,419 and 100% of the events. The modal also includes a 'Selected' dropdown set to 'Yes' and a 'Next >' button. The bottom of the screen shows the Windows taskbar with the search bar and various application icons.

Search Results Summary:

| Field | Count | % |
|-----------|-------|------|
| target-PC | 2,419 | 100% |

Timeline format ▾ — Zoom Out

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a source 4
- a sourcetype 4

INTERESTING FIELDS

- a ComputerName 2

source

4 Values, 100% of events Selected

Reports

- Top values
- Top values by time
- Rare values

[Events with this field](#)

| Values | Count | % |
|---|-------|---------|
| WinEventLog:Security | 1,212 | 50.103% |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | 585 | 24.184% |
| WinEventLog:System | 346 | 14.303% |
| WinEventLog:Application | 276 | 11.41% |

8' /></System><EventData><Data Name='RuleName'>technique_id=T1036,

✓ 2,419 events (02/09/2025 07:00:00.000 to 03/09/2025 07:23:26.000) Job ▾ || ↶ ↷ ⬇ ⚡ Smart

No Event Sampling ▾

Events (2,419) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a source 4
- a sourcetype 4

INTERESTING FIELDS

- a ComputerName 2

sourcetype

4 Values, 100% of events Selected

Reports

- Top values
- Top values by time
- Rare values

[Events with this field](#)

| Values | Count | % |
|---|-------|---------|
| WinEventLog:Security | 1,212 | 50.103% |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | 585 | 24.184% |
| WinEventLog:System | 346 | 14.303% |
| WinEventLog:Application | 276 | 11.41% |

8' /></System><EventData><Data Name='RuleName'>technique_id=T1036, tec

Buscar

Servidor:

La ip pertenece al servidor splunk instalado

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP

192.168.1.137 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

Cancel Back Next

Descargamos sysmon:

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

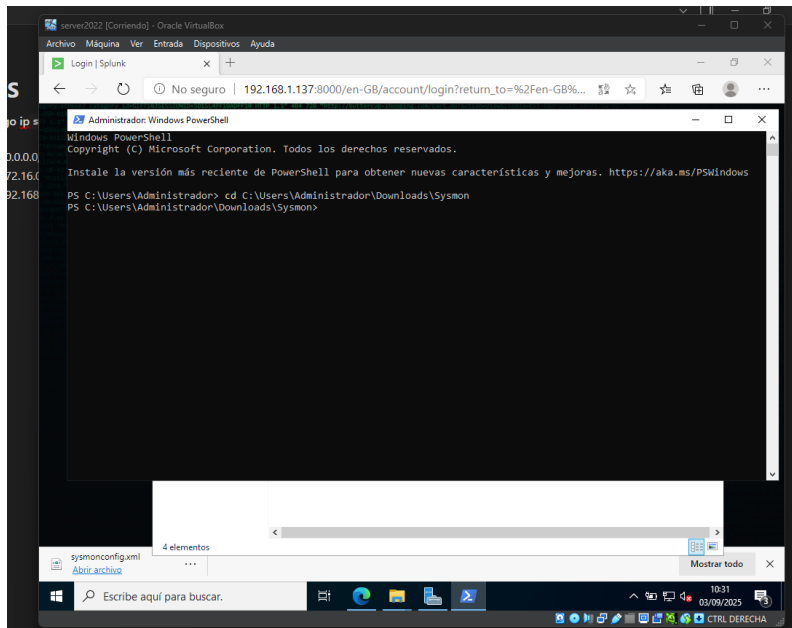
también el archivo de configuración sysmon olaf :

<https://github.com/olafhartong/sysmon-modular> pero usamos el archivo:

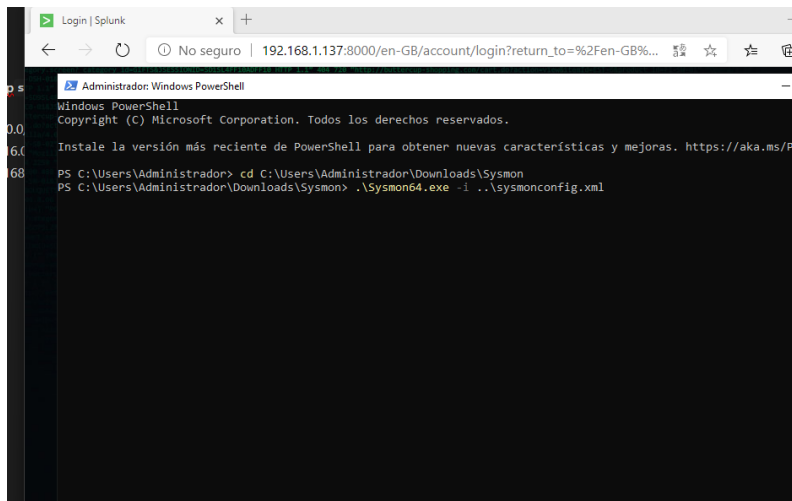
<https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml>

clic en raw y guardamos el archivo

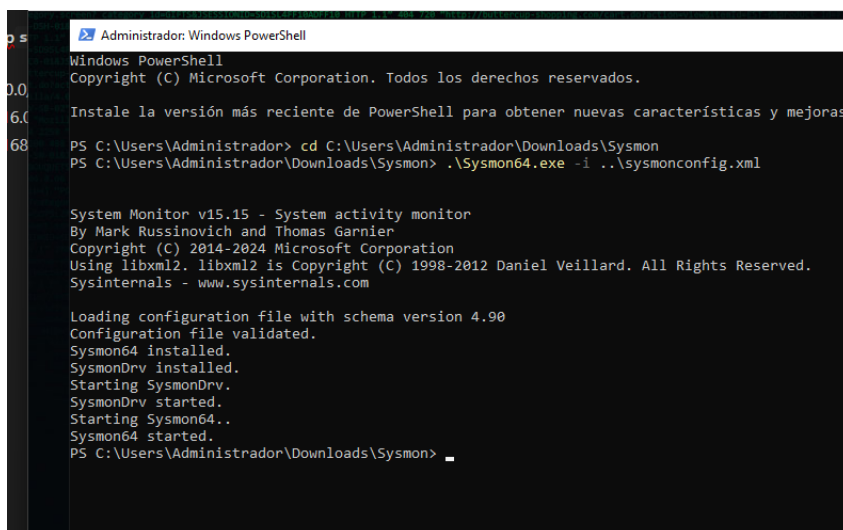
una vez descomprimo el archivo de sysmon , copiamos la ruta y vamos a PowerShell como administrador



Vamos a la siguiente ruta:



E instalamos sysmon



Configuraremos un archivo inputs.conf (c:\program Files\splunkUniversalForwarder\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\splunkUniversalForwarder\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 forwarder 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

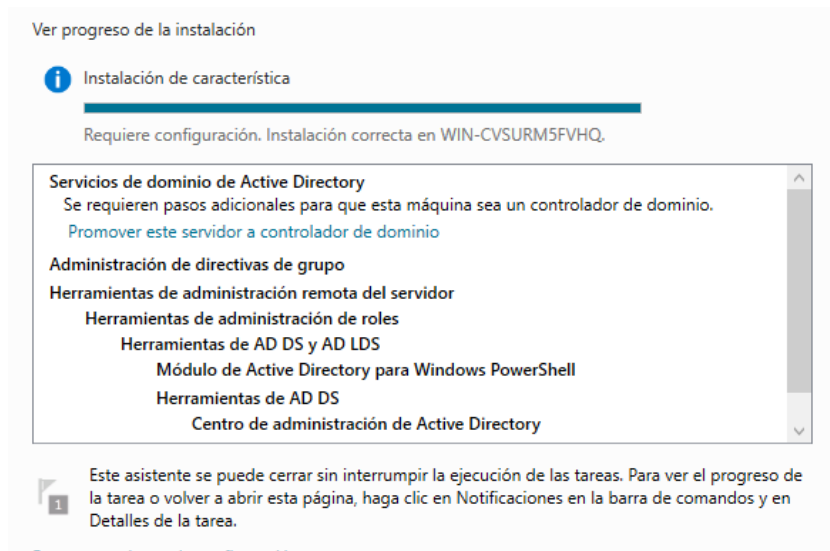
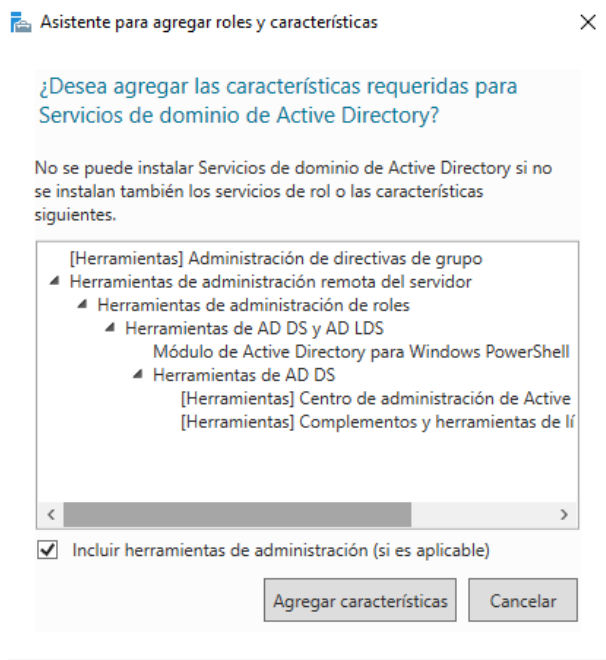
[WinEventLog://System]
index = endpoint
disabled = false

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

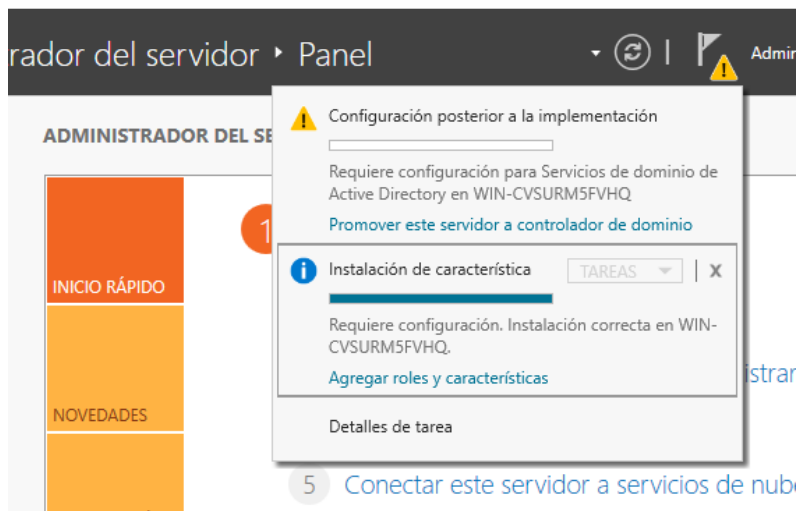
Una vez guardado a la copia reiniciamos el servicio de splunk forwarder

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

| Indexes | | | | | | | | | |
|---|---------------------------|--------|-------------|------|--------|-------|------------|-------------------|---------------------|
| A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more | | | | | | | | | |
| 16 Indexes | filter | | 20 per page | | | | | | |
| endpoint | Edit Delete Disable | Events | search | 3 MB | 500 GB | 10.9K | 2 days ago | a few seconds ago | \$SPLUNK B/endpoint |



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



Será el top level nivel

Seleccionar la operación de implementación

☐ Agregar un controlador de dominio a un dominio existente

☐ Agregar un nuevo dominio a un bosque existente

☒ Agregar un nuevo bosque

Especificar la información de dominio para esta operación

Nombre de dominio raíz:

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

Rutas de acceso

SERVIDOR DE DESTINO
WIN-CVSURM5FVHQ

Configuración de implem...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Especificar la ubicación de la base de datos de AD DS, archivos de registro y SYSVOL

Carpeta de la base de datos: ...

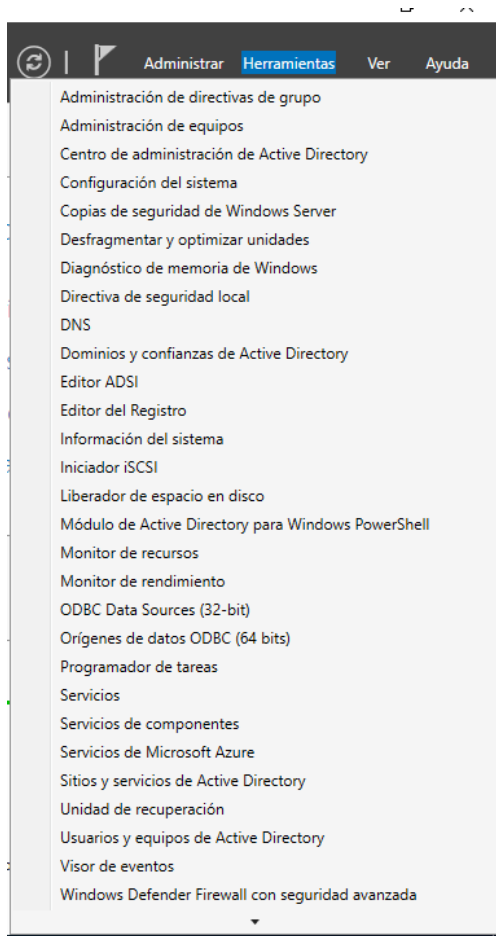
Carpeta de archivos de registro: ...

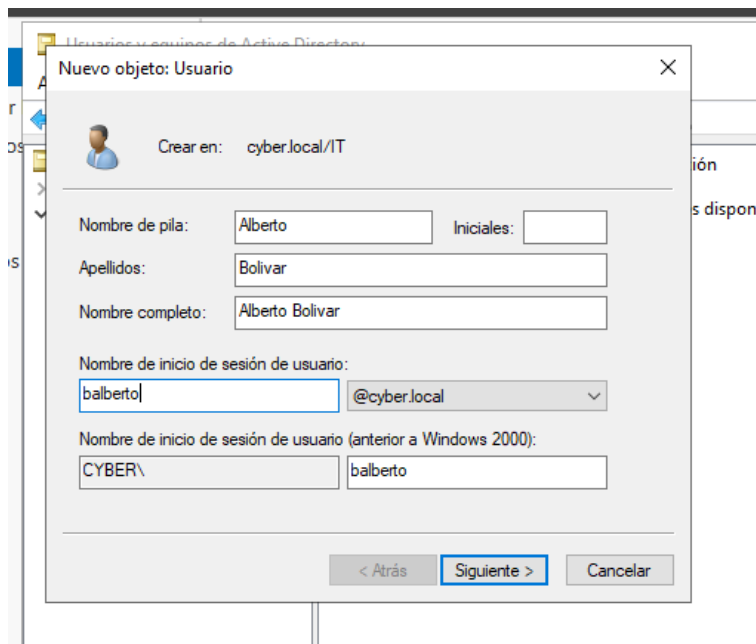
Carpeta SYSVOL: ...

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



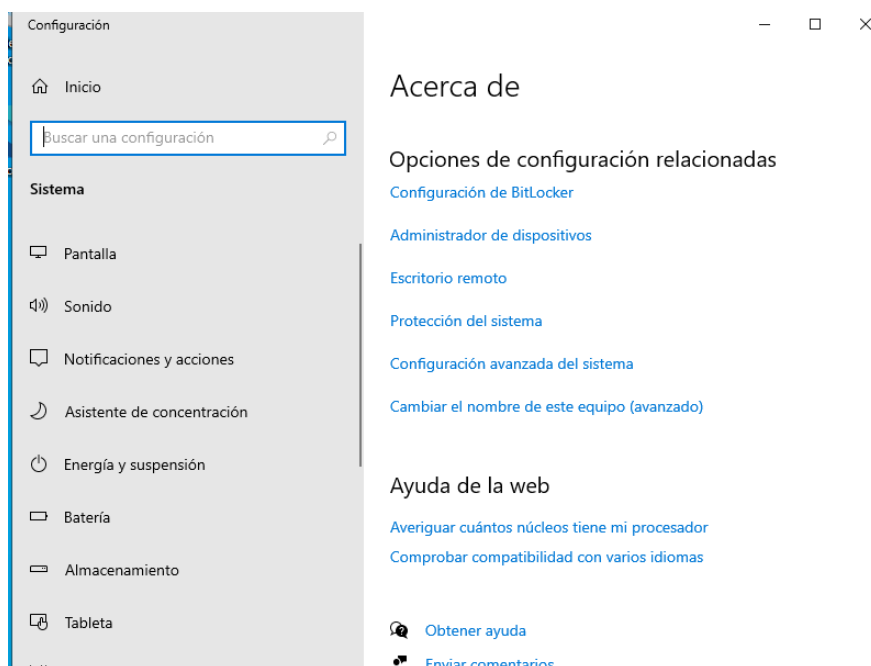
Usuarios y equipos de active directory



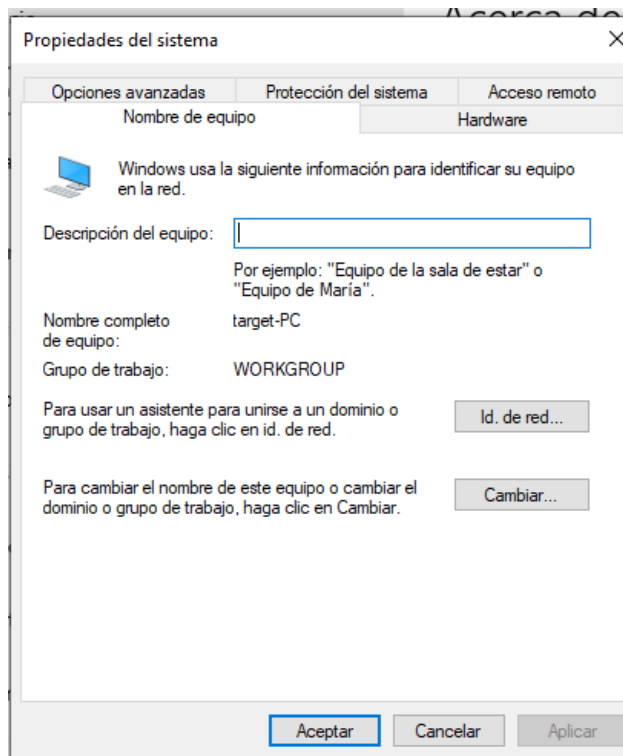


Ahora necesitamos unir nuestro pc normal al controlador de dominio del servidor

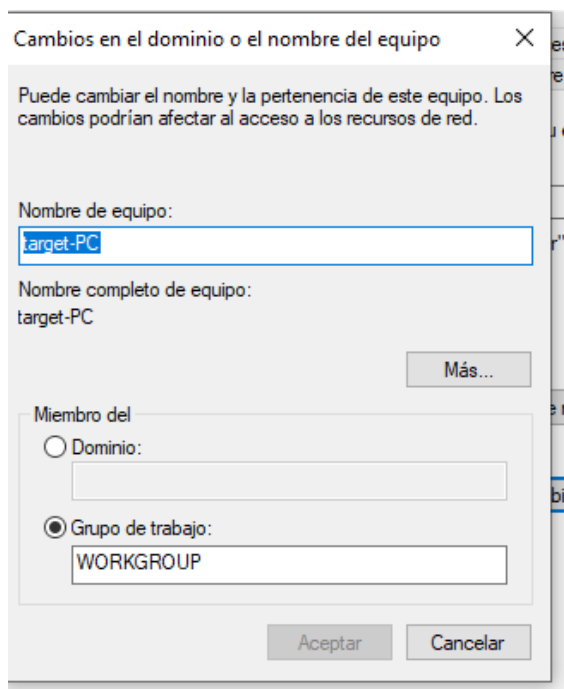
Barra de búsqueda: pc-→ propiedades-→

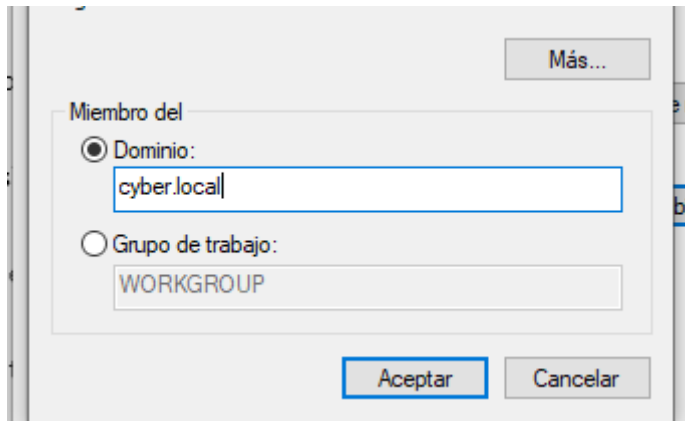


Configuración avanzada del sistema→ nombre equipo

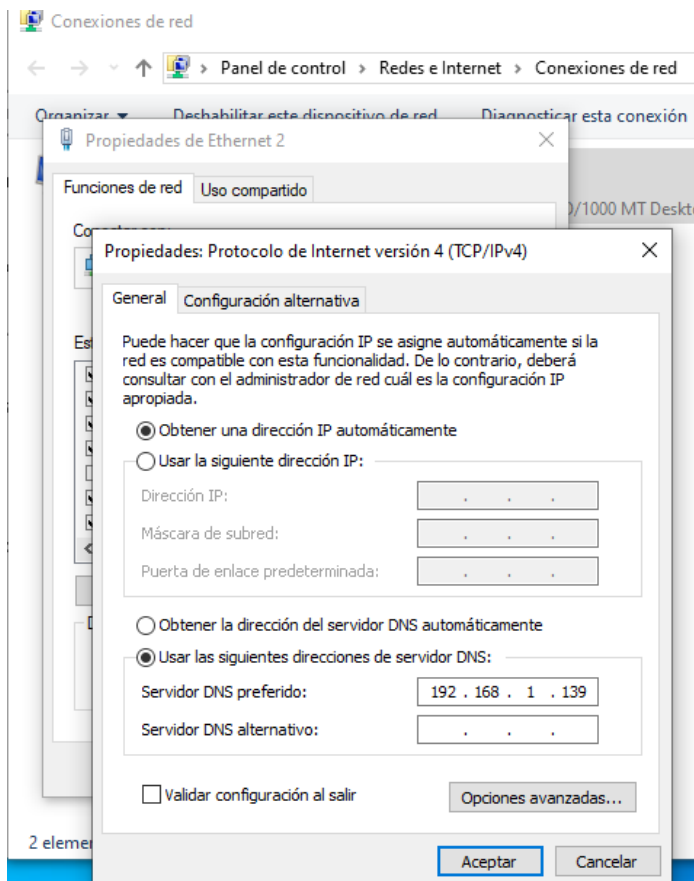


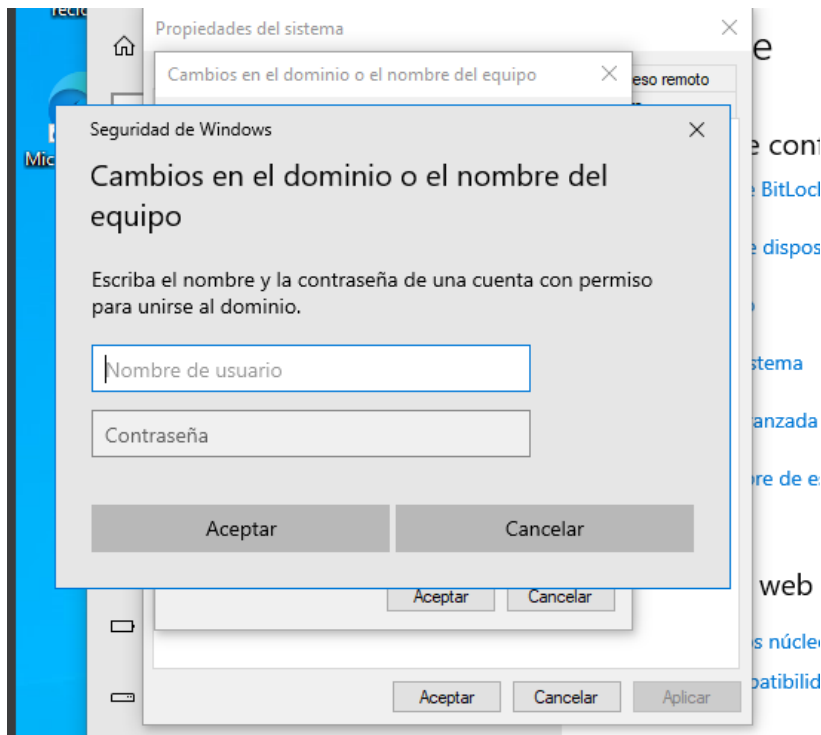
Cambiar→miembro del: y escribimos el nombre del dominio



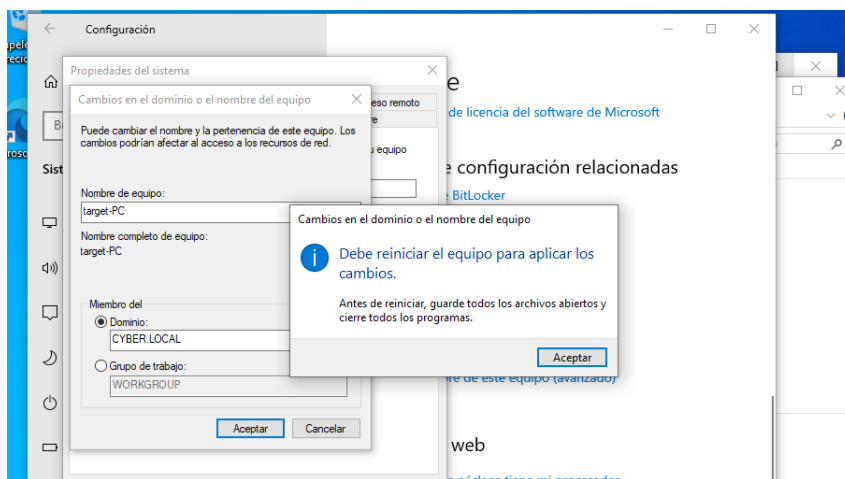


Al intentar agregarlo da un error ya que el pc no podría resolver el nombre de dominio dns, entonces tendríamos que configurarlo manualmente agregando el del servidor





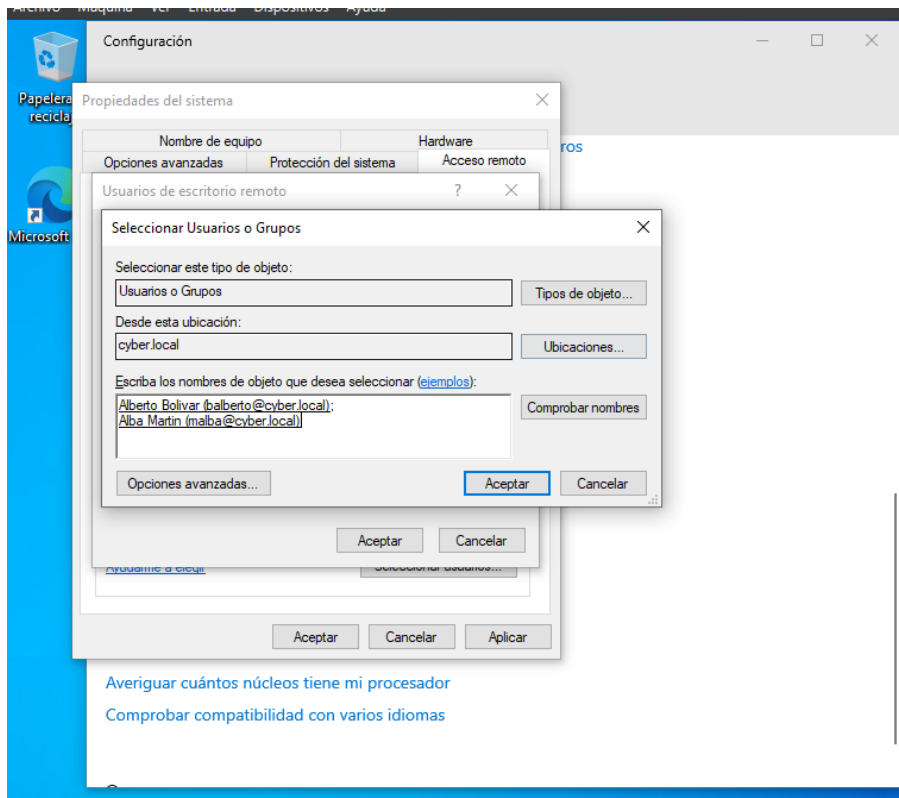
Usaremos la cuenta del administrador del servidor



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



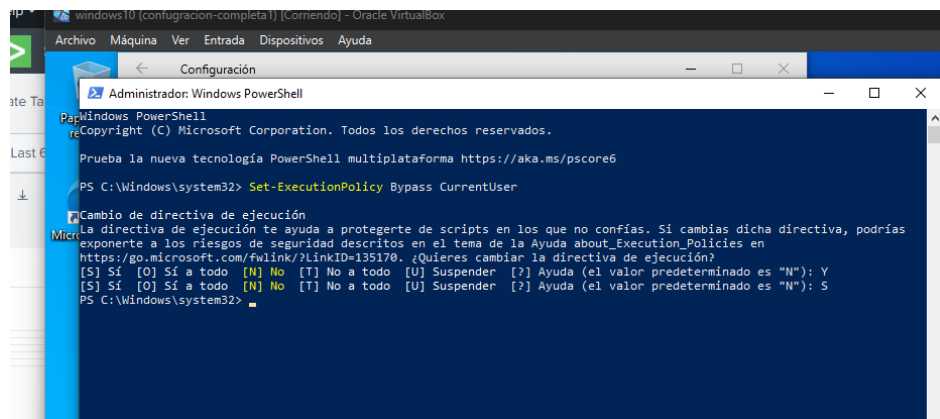
Una vez hecho todo esto procederemos a iniciar sesión con nuestro administrador en el target pc y habilitaremos el rdp para que los usuarios puedan acceder



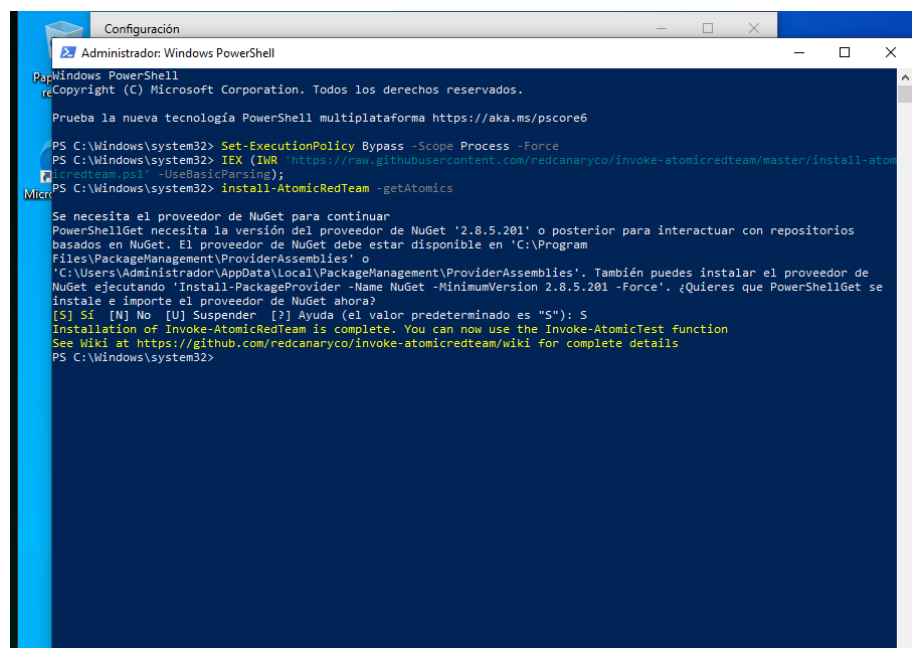
Ya con todo instalado y seteado, se puede hacer diferentes cosas para generar telemetría, como fuerzas brutas, ataques de phishing y demás.

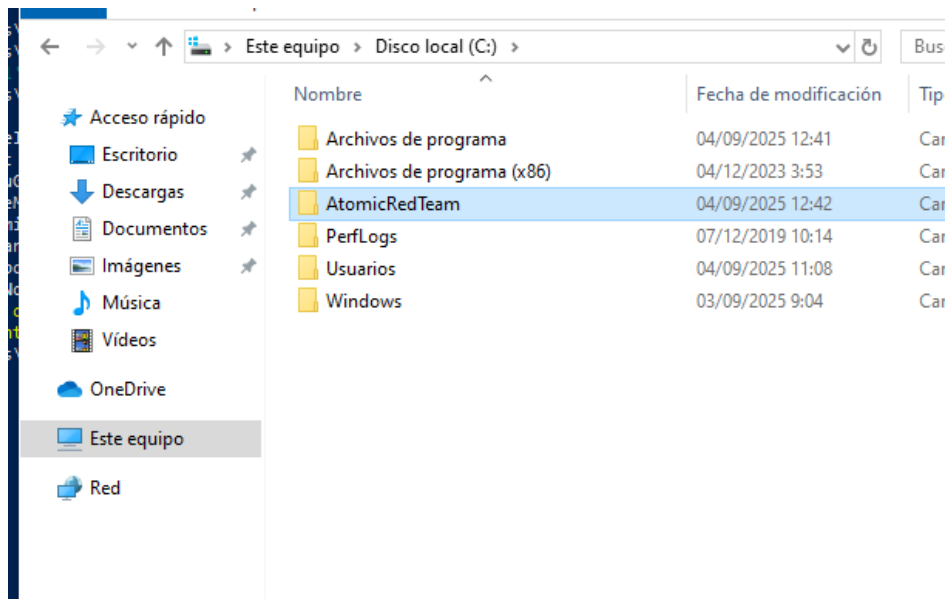
Instalar atomic red team

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

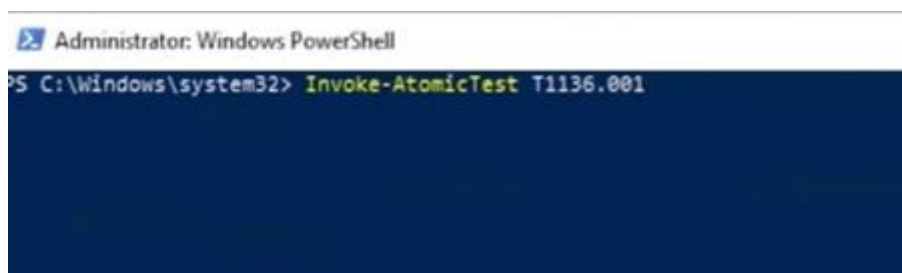


Hay que excluir la carpeta disco c: en el antivirus de Windows defender





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



Y de esa manera verificar la telemetría

