



**Certificado de Profesionalidad en
Seguridad Informática
IronHack - SOC**

**Módulo 3
Gestión de Incidentes
Práctica 3 - Splunk**

Alumno: Julián Gordon

Indice

Enunciado.....	3
Introducción.....	4
Instalación de Splunk en Entorno Local.....	5
Instalación y Configuración de Sysmon en Máquina Windows.....	10
Configuración de Splunk para Recibir Eventos de Sysmon.....	24
Configuración de Data Inputs.....	26
Generación de Eventos de Seguridad.....	33
Análisis de Eventos en Splunk.....	35
Conclusiones.....	37

Enunciado

1. Instalación de Splunk en Entorno Local

Descarga de Splunk: Accede al sitio web de Splunk y crea una cuenta (si no tienes una). Descarga la versión gratuita de Splunk para tu sistema operativo (Windows/Linux/Mac). Instalación de Splunk: Sigue las instrucciones de instalación específicas para tu sistema operativo. Durante la instalación, configura un nombre de usuario y una contraseña para el acceso al dashboard de Splunk. Inicio de Splunk: Inicia el servicio de Splunk y accede al dashboard a través de tu navegador web (por defecto en <http://localhost:8000>).

2. Instalación y Configuración de Sysmon en Máquina Windows

Descarga de Sysmon: Descarga Sysmon desde el sitio web de Microsoft Sysinternals. Instalación de Sysmon: Abre una consola de comandos con privilegios de administrador. Instala Sysmon utilizando el comando: Verificación de Instalación: Verifica que Sysmon está funcionando y generando eventos en el visor de eventos de Windows.

3. Configuración de Splunk para Recibir Eventos de Sysmon

Configuración de Data Inputs en Splunk: Desde el dashboard de Splunk, navega a "Settings" > "Data Inputs" > "Local Event Log Collection". Configura Splunk para recibir eventos de los logs generados por Sysmon (normalmente bajo "Microsoft-Windows-Sysmon/Operational"). Verificación de Recepción de Eventos: Asegúrate de que Splunk está recibiendo los eventos de Sysmon correctamente revisando los índices de datos en el dashboard de Splunk.

4. Generación de Eventos de Seguridad

Máquina Windows: Genera varios intentos de inicio de sesión fallidos. Ejecuta varias aplicaciones, para visualizar los eventos de apertura de aplicación.

5. Análisis de Eventos en Splunk

Creación de Búsquedas y Alertas: Utiliza el lenguaje de búsqueda de Splunk (SPL) para crear consultas que identifiquen eventos específicos de Sysmon. Configura una alerta en Splunk para identificar la apertura de aplicaciones concretas.

6. Documentación del Proceso

Compila todas las capturas de pantalla en un documento. Redacta una breve descripción para cada paso, explicando el proceso seguido y los resultados obtenidos. Asegúrate de incluir cualquier problema encontrado y cómo se resolvió.

Introducción

En este ejercicio práctico, exploramos la instalación, configuración y utilización de dos herramientas fundamentales en el ámbito de la seguridad informática y el análisis de logs: Splunk y Sysmon. Splunk es una plataforma líder en análisis de datos operativos y de seguridad, mientras que Sysmon, una herramienta desarrollada por Microsoft Sysinternals, es ampliamente utilizada para monitorear la actividad del sistema en entornos Windows.

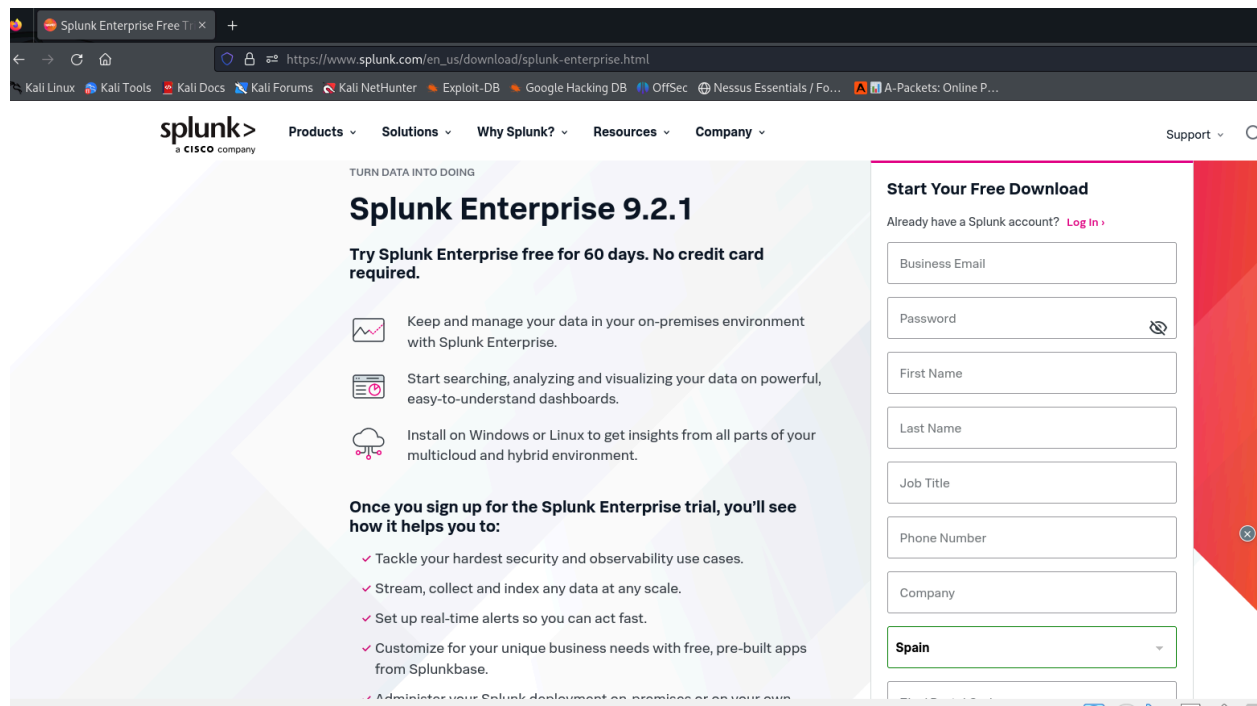
El objetivo principal de esta práctica fue implementar un entorno de monitoreo de seguridad local, donde Splunk sirvió como la plataforma central para la recolección, indexación y análisis de eventos de seguridad generados por Sysmon en una máquina Windows. A lo largo del ejercicio, seguimos una serie de pasos que abarcan desde la instalación inicial de Splunk y Sysmon hasta la configuración de alertas en Splunk para detectar eventos específicos de seguridad, como la apertura de PowerShell.

A través de la configuración de Splunk para recibir eventos de Sysmon, la generación de eventos de seguridad en la máquina Windows y el análisis de estos eventos en Splunk, obtuvimos una comprensión práctica de cómo implementar una solución efectiva de monitoreo de seguridad utilizando estas herramientas populares. La práctica también incluye la documentación detallada de cada paso realizado, lo que proporciona un recurso valioso para futuras referencias y aprendizaje continuo en el campo de la ciberseguridad y el análisis de logs.

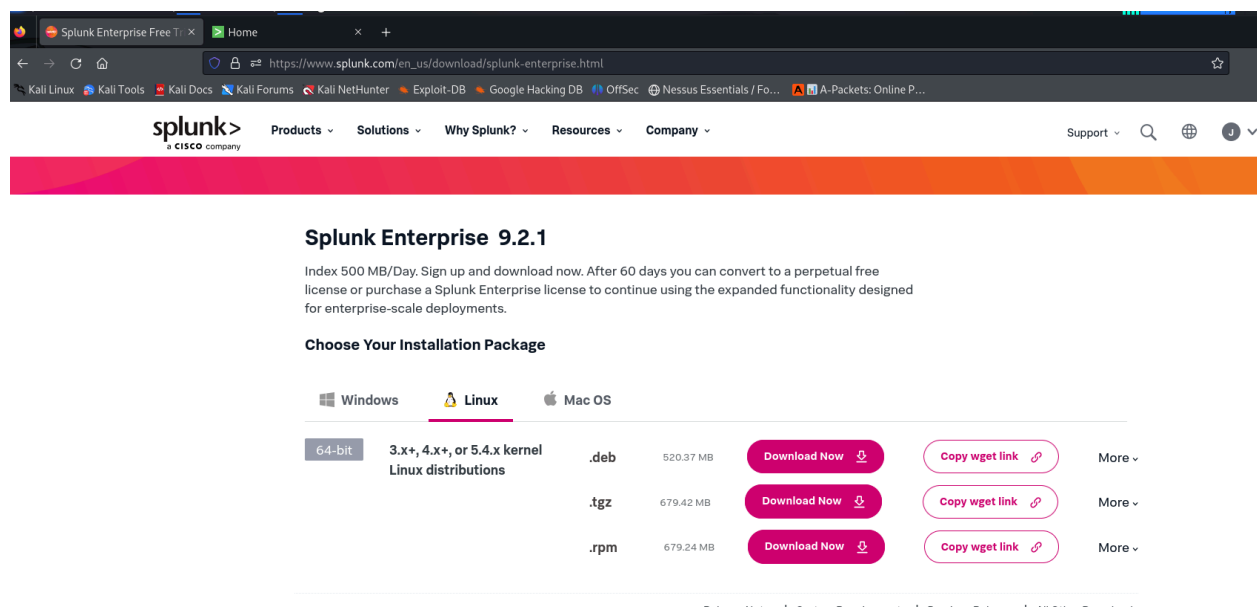
Este informe presenta un resumen exhaustivo de los pasos realizados durante la práctica, destacando los principales puntos de configuración, los resultados obtenidos y las lecciones aprendidas en el proceso. Además, ofrece una visión general de las alertas activadas, una característica fundamental en la detección temprana y la respuesta a incidentes en entornos de ciberseguridad.

Instalación de Splunk en Entorno Local

Comenzaremos esta práctica ingresando en nuestra máquina virtual de Kali Linux, abriendo un navegador y creando una cuenta en Splunk, en su página oficial.



Una vez tenemos la cuenta creada, descargamos Splunk de la página web oficial.



Seleccionamos la opción .deb que es la adecuada para Kali Linux.

Una vez tengamos descargado el paquete .deb, abriremos una terminal, elevamos permisos a usuario root, vamos a la carpeta /home/kali/Downloads y ejecutamos el siguiente comando: dpkg -i [nombre del fichero descargado de splunk-9.2.1..]

```
(kali㉿kali)-[~/Downloads]
└─$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~/Downloads]
└─# ls
'Codigo activacion Nessus'      Nessus-10.7.2-debian10_amd64.deb      ZAP_2_14_0_unix.sh
coreruleset                    splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Nessus-10.7.2-debian10_amd64    splunkforwarder-9.2.1-78803f08aabb-Linux-armv8.deb

(kali㉿kali)-[~/Downloads]
└─# dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 420827 files and directories currently installed.)
Preparing to unpack splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
```

Esto iniciará la instalación de Splunk. Una vez termine, iremos a la carpeta /opt/Splunk/bin.

```
(root㉿kali)-[/opt/splunk]
└─# cd bin

(root㉿kali)-[/opt/splunk/bin]
└─# ls
```

Desde allí ejecutaremos el comando ./splunk start

```
(root㉿kali)-[/opt/splunk/bin]
└─# ./splunk start
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021
```

Aceptamos las licencias y luego nos pedirá un nombre de usuario y una contraseña. En este caso vamos a usar `splunk_admin` de username.

```
"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]: y
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: splunk_admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
```

Esto una vez que lo tengamos activo, nos dirá la ubicación de donde se está ejecutando <http://kali:8000> en nuestro caso.

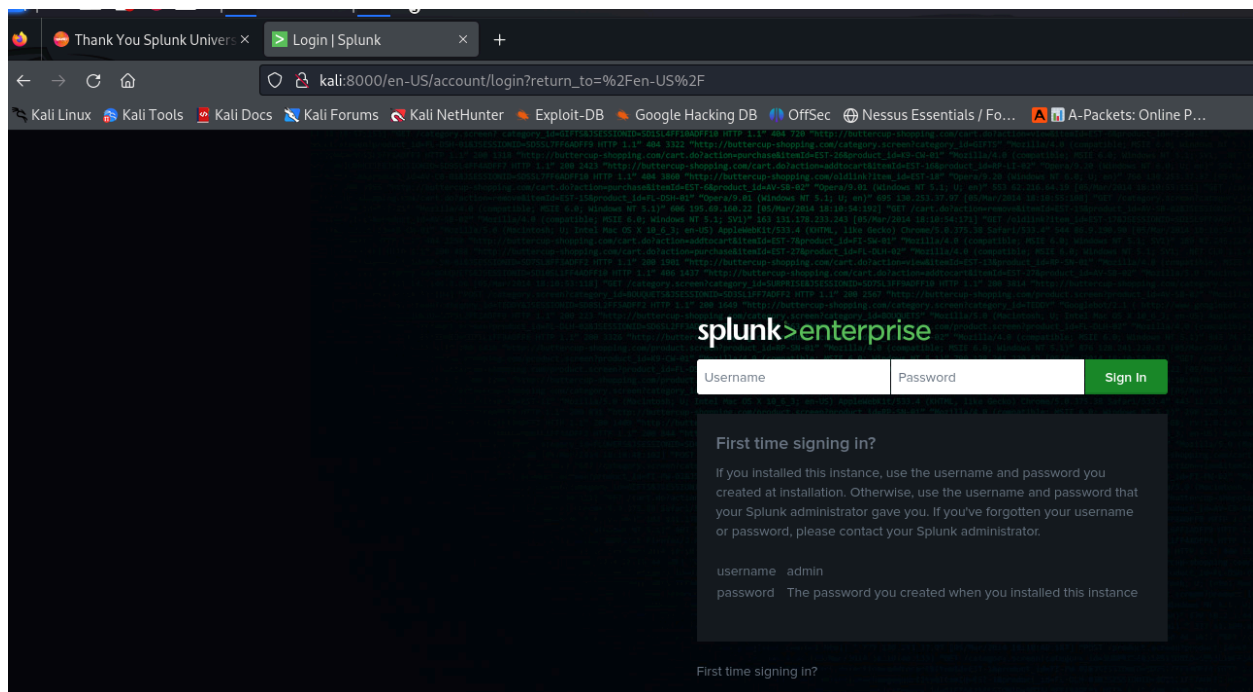
```
Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

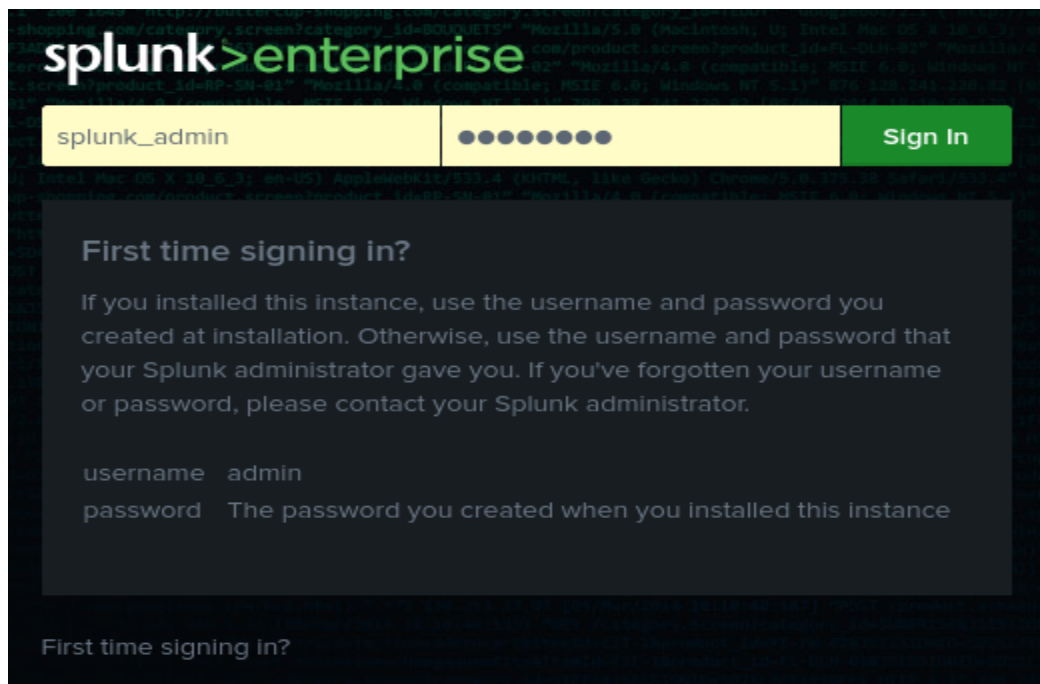
The Splunk web interface is at http://kali:8000

(root@kali)-[/opt/splunk/bin]
```

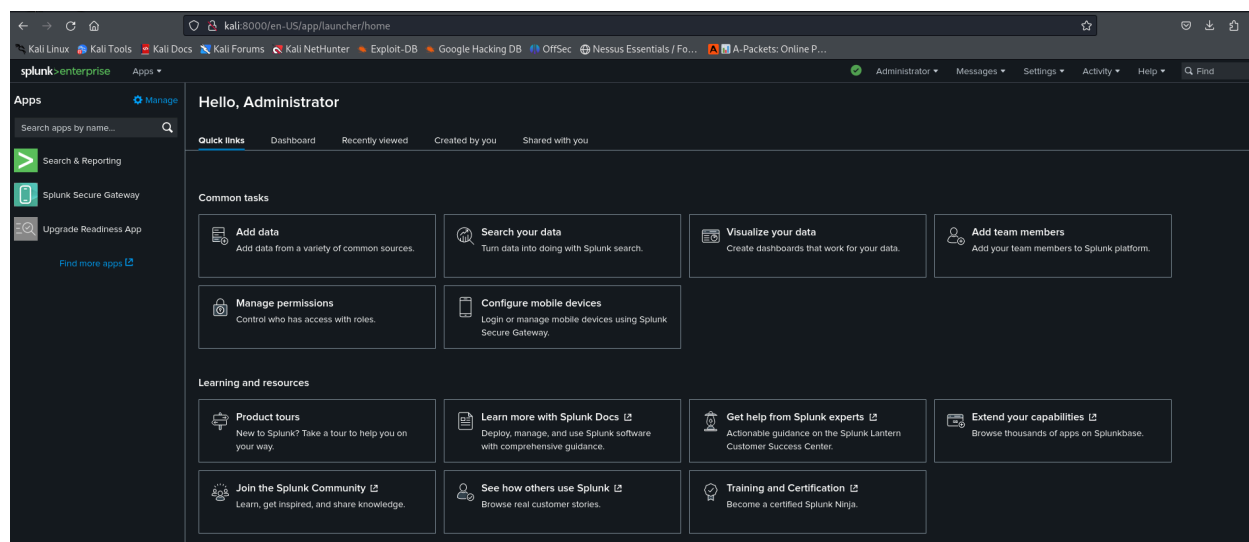
Ahora abriremos nuestro navegador y accederemos a <http://kali:8000>



Pondremos las credenciales que creamos inicialmente en la instalación.



Una vez accedemos, el panel de control se verá así:



Instalación y Configuración de Sysmon en Máquina Windows

El siguiente paso será abrir nuestra máquina virtual de Windows 10 y verificar que ambas máquinas están en la misma red. Para ello desde Windows abrimos un cmd y ejecutamos ipconfig, una vez nos da la nuestra IP, vamos a Kali Linux y desde la terminal hacemos ping a la IP de Windows 10. Luego ejecutamos ifconfig y desde la máquina de Windows10 hacemos un ping a la de Kali. Podemos verificar que están en la misma red.

```
(root@kali)-[/opt/splunk/bin]
# ping 10.0.2.30
PING 10.0.2.30 (10.0.2.30) 56(84) bytes of data.
64 bytes from 10.0.2.30: icmp_seq=1 ttl=128 time=1.19 ms
64 bytes from 10.0.2.30: icmp_seq=2 ttl=128 time=1.70 ms
64 bytes from 10.0.2.30: icmp_seq=3 ttl=128 time=1.44 ms
^C
— 10.0.2.30 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.188/1.443/1.699/0.208 ms
```

```
Adaptador de Ethernet LAN:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::4707:e92d:9f63:d139%10
    Dirección IPv4. . . . . : 10.0.2.30
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.1

Adaptador de Ethernet Ethernet:

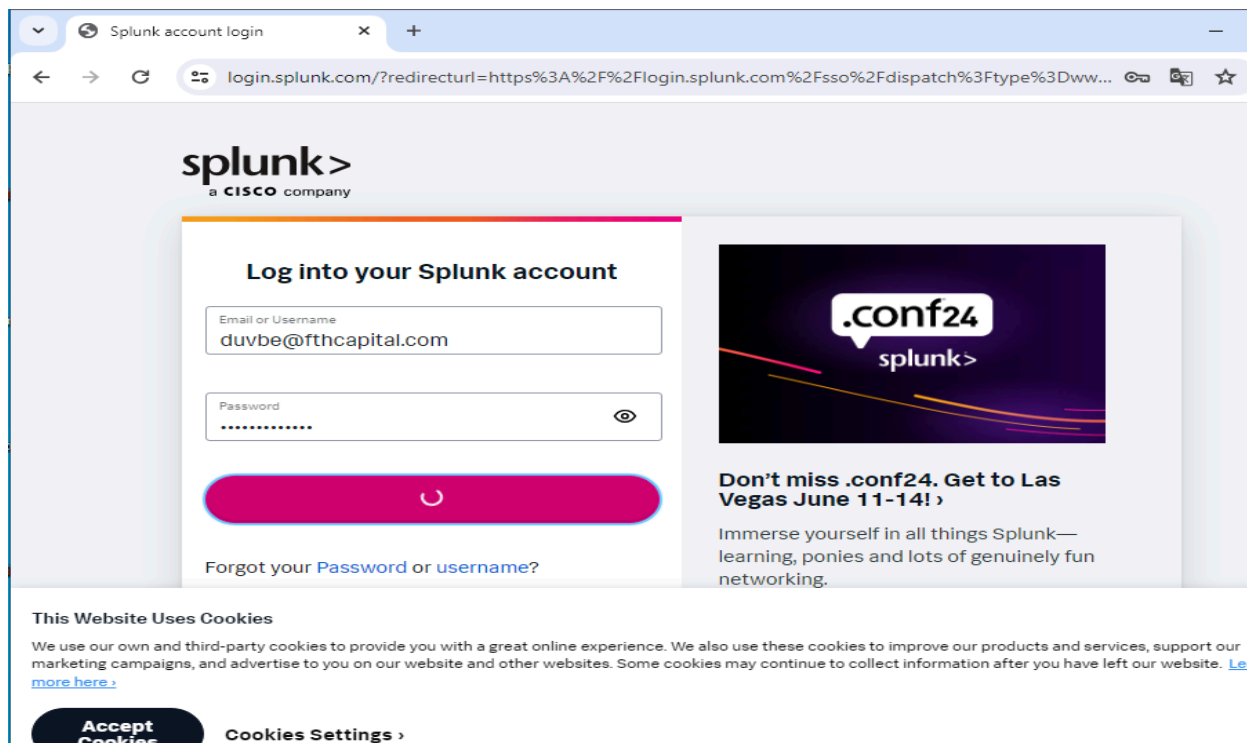
    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::3a03:b87b:e28a:c218%6
    Dirección IPv4. . . . . : 192.168.56.103
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.10.100

C:\Users\Admin>ping 10.0.2.26

Haciendo ping a 10.0.2.26 con 32 bytes de datos:
Respuesta desde 10.0.2.26: bytes=32 tiempo=5ms TTL=64

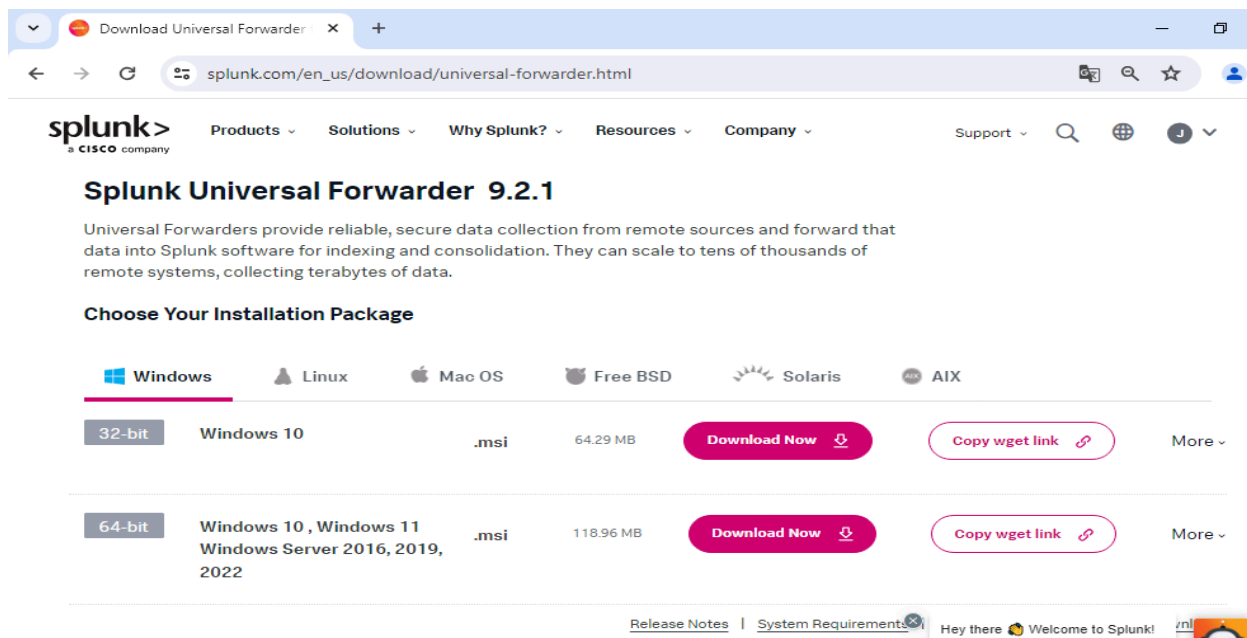
Estadísticas de ping para 10.0.2.26:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 5ms, Máximo = 5ms, Media = 5ms
Control-C
^C
C:\Users\Admin>
```

Una vez que verificamos que están conectadas correctamente, iremos a nuestra máquina de Windows10 y descargamos e instalamos Splunk Universal Forwarder 9.2.1.msi de 64 bit. Para ello primero debemos hacer login en la página web y desde allí descargarlo.

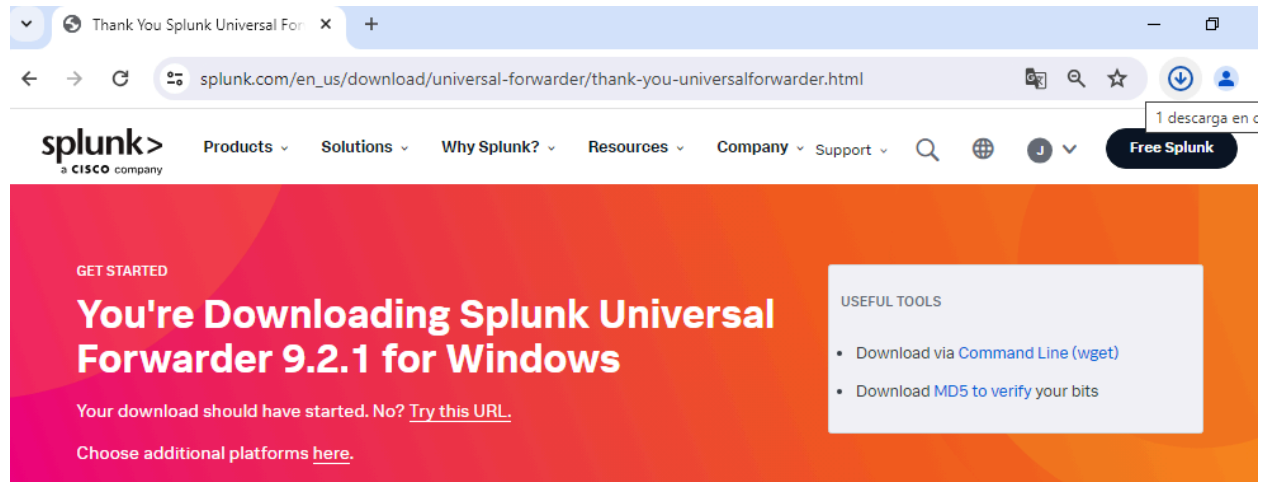


Seleccionamos Splunk Universal Forwarder para Windows 64-bit y descargamos.

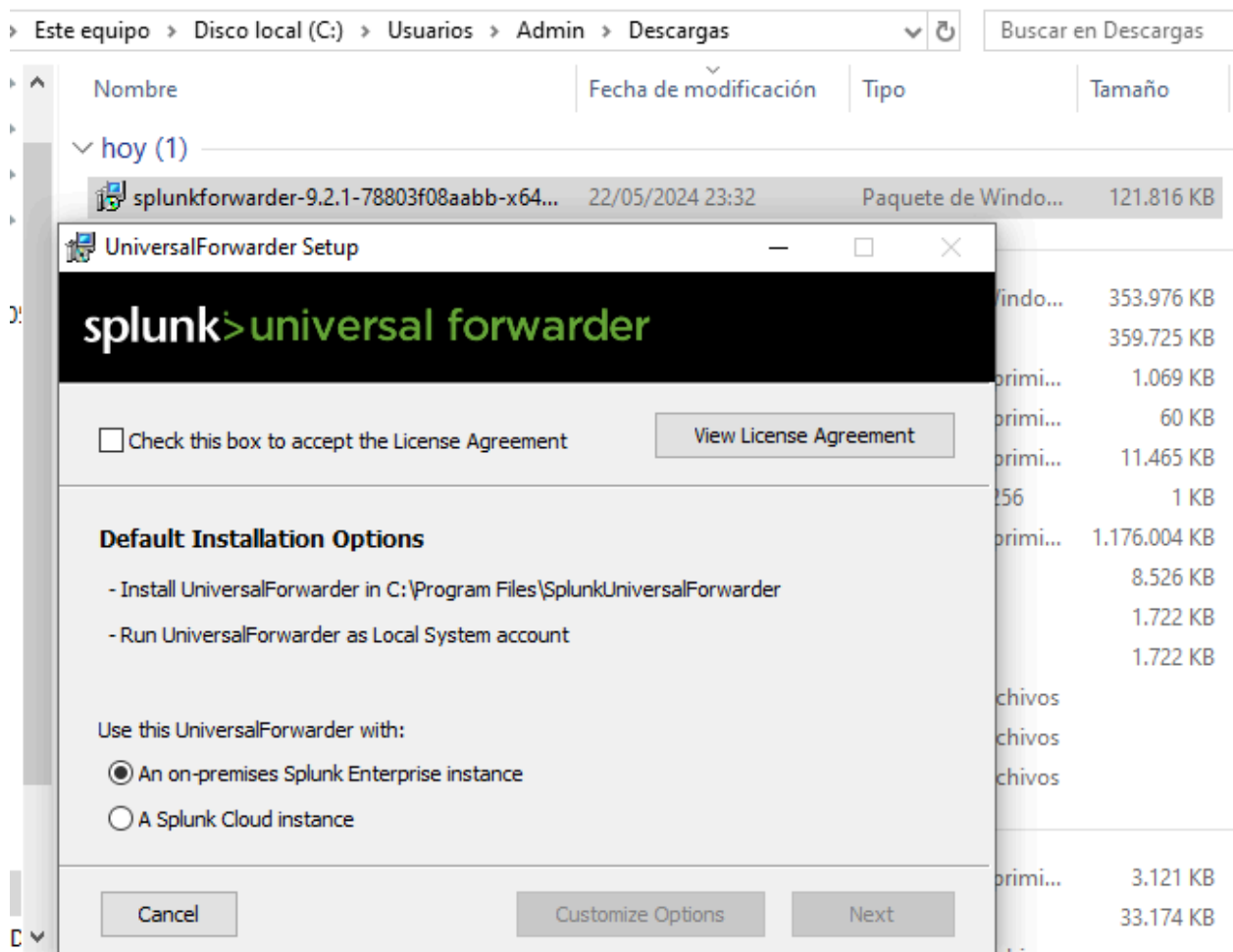
S



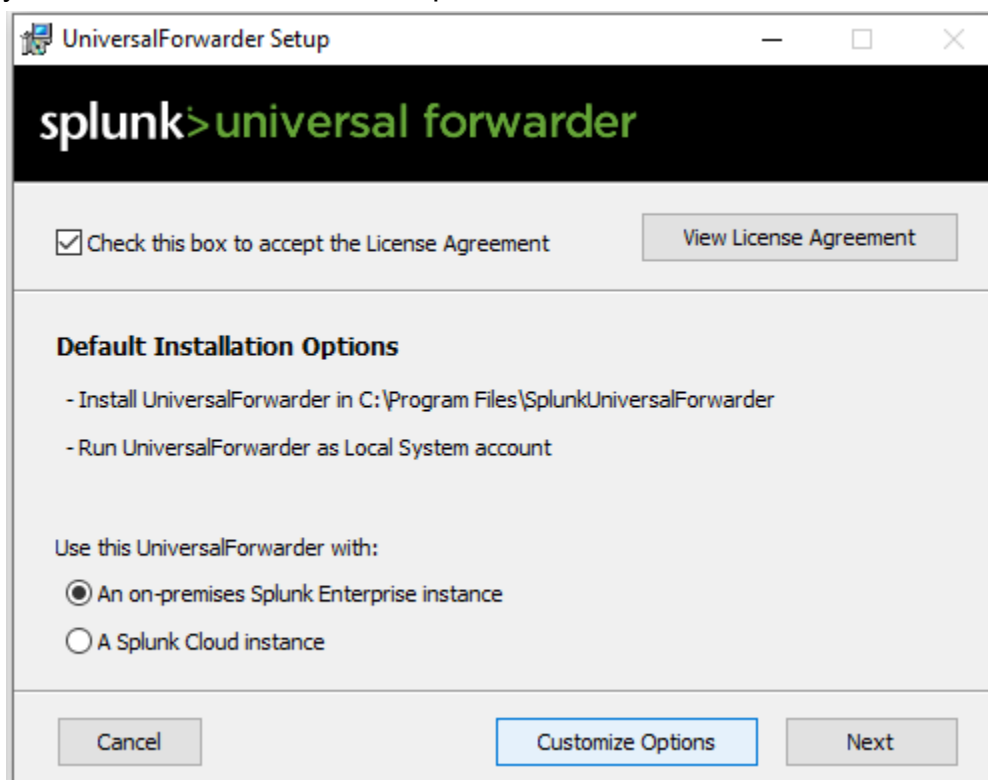
Empezará a descargar el fichero .msi.



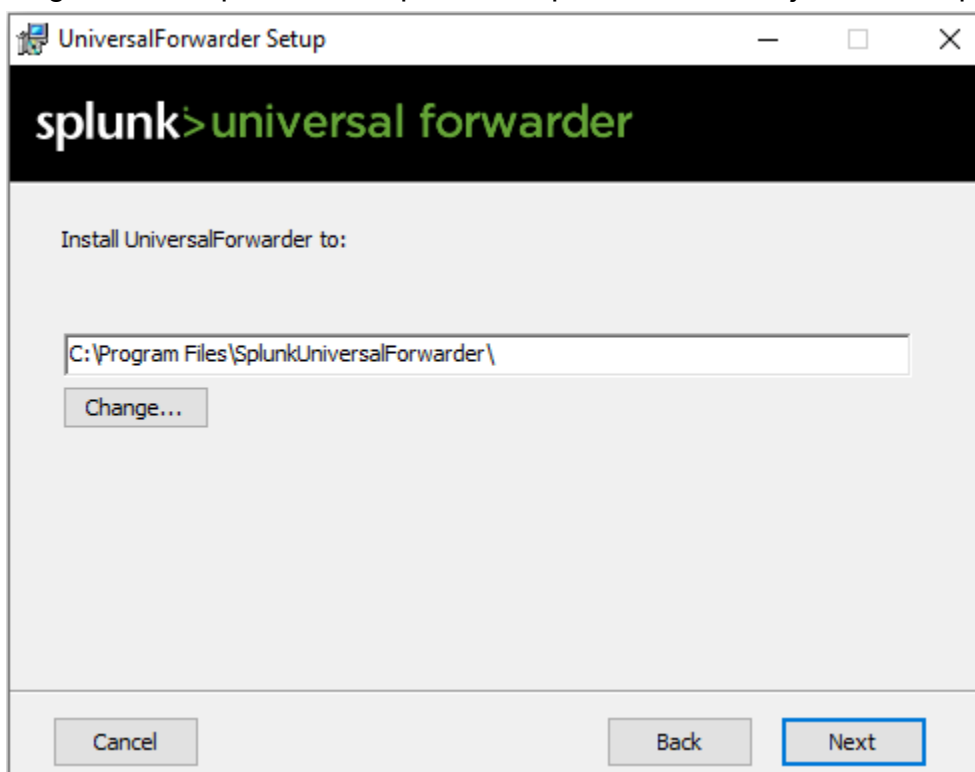
Una vez terminada la descarga, abrimos el fichero descargado.



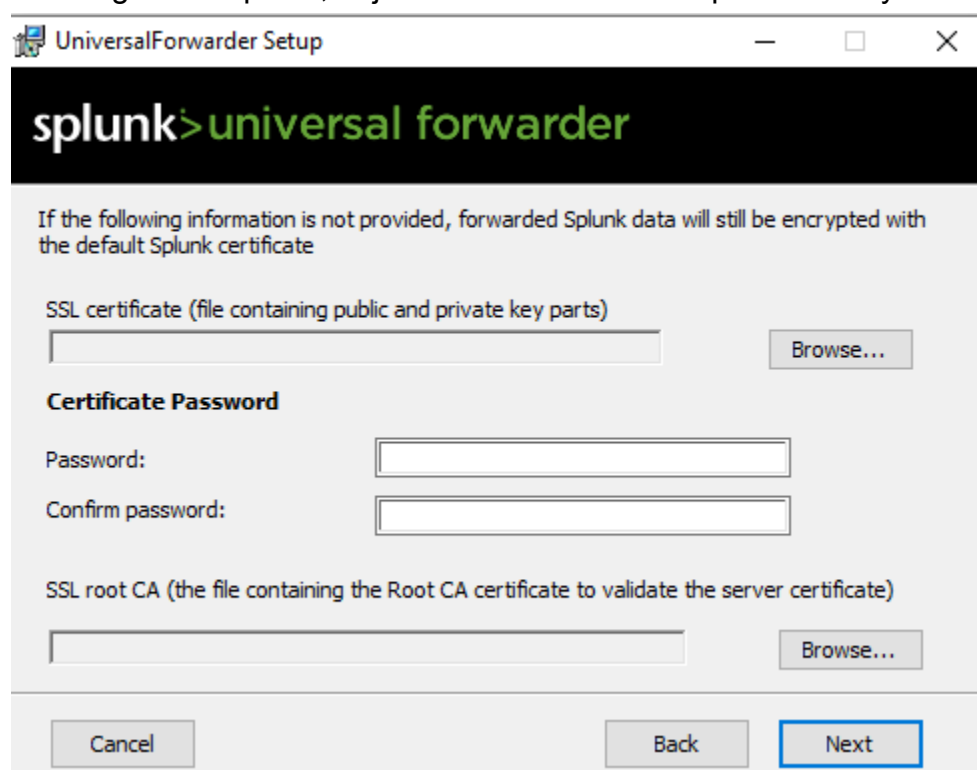
Podemos observar que se inicia la configuración de instalación. Aceptamos la Licencia y seleccionamos Customize Options



Elegimos la carpeta donde queremos que se instale, dejaremos la que está por defecto.

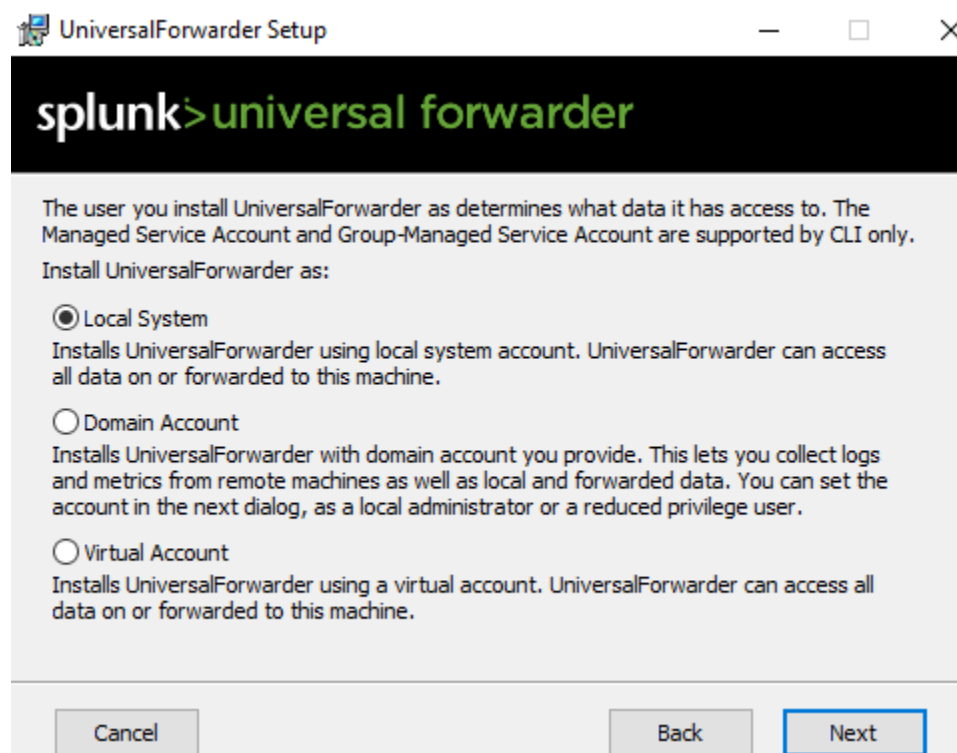


En la siguiente opción, dejamos todo como viene por defecto y avanzamos.



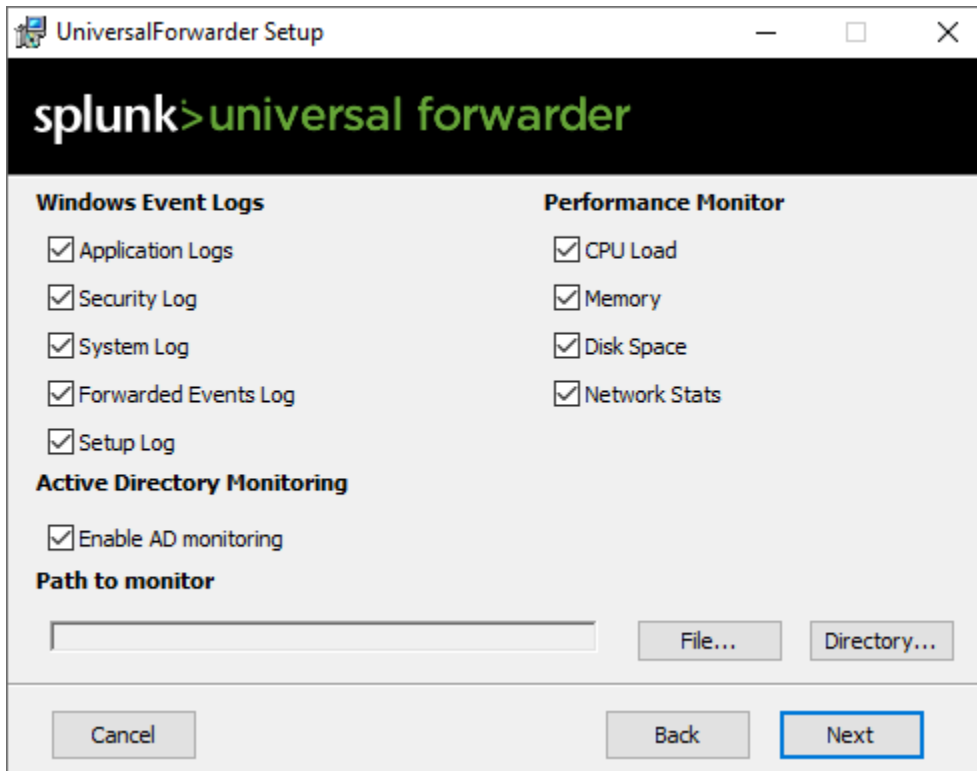
The screenshot shows the 'UniversalForwarder Setup' window. At the top is the 'splunk>universal forwarder' logo. Below it, a message states: 'If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate'. The main section contains three fields: 'SSL certificate (file containing public and private key parts)' with a text box and a 'Browse...' button; 'Certificate Password' with 'Password:' and 'Confirm password:' labels and corresponding text boxes; and 'SSL root CA (the file containing the Root CA certificate to validate the server certificate)' with a text box and a 'Browse...' button. At the bottom are 'Cancel', 'Back', and 'Next' buttons, with 'Next' being the active button.

Seleccionamos Local System, qué será la forma en la cual lo usaremos.



The screenshot shows the 'UniversalForwarder Setup' window at the second step. It features the same 'splunk>universal forwarder' logo. The text explains: 'The user you install UniversalForwarder as determines what data it has access to. The Managed Service Account and Group-Managed Service Account are supported by CLI only. Install UniversalForwarder as:'. There are three radio button options: 'Local System' (which is selected), 'Domain Account', and 'Virtual Account'. Each option has a descriptive paragraph below it. At the bottom are 'Cancel', 'Back', and 'Next' buttons, with 'Next' being the active button.

Seleccionamos todas las opciones disponibles.



The screenshot shows the 'UniversalForwarder Setup' window. At the top is the 'splunk>universal forwarder' logo. Below it, there are two columns of checkboxes. The left column is titled 'Windows Event Logs' and includes 'Application Logs', 'Security Log', 'System Log', 'Forwarded Events Log', and 'Setup Log'. The right column is titled 'Performance Monitor' and includes 'CPU Load', 'Memory', 'Disk Space', and 'Network Stats'. Below these is a section for 'Active Directory Monitoring' with a checkbox for 'Enable AD monitoring'. Underneath is a 'Path to monitor' section with a text input field and two buttons: 'File...' and 'Directory...'. At the bottom are three buttons: 'Cancel', 'Back', and 'Next'.

Windows Event Logs

- ☒ Application Logs
- ☒ Security Log
- ☒ System Log
- ☒ Forwarded Events Log
- ☒ Setup Log

Performance Monitor

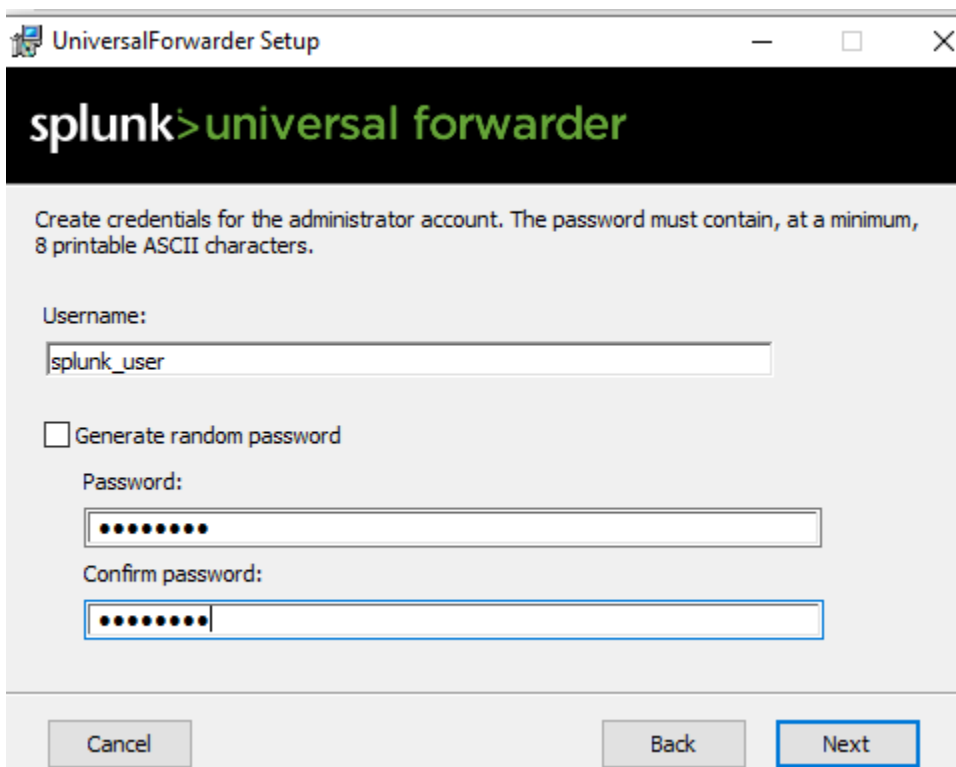
- ☒ CPU Load
- ☒ Memory
- ☒ Disk Space
- ☒ Network Stats

Active Directory Monitoring

- ☒ Enable AD monitoring

Path to monitor

Ahora creamos usuario `splunk_user` y contraseña la que venimos usando en ejercicios anteriores, `P@ssw0rd`.



The screenshot shows the 'UniversalForwarder Setup' window at the credential creation step. It features the 'splunk>universal forwarder' logo and a message: 'Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.' Below this is a 'Username:' label followed by a text input field containing 'splunk_user'. There is an unchecked checkbox for 'Generate random password'. Below that is a 'Password:' label followed by a password input field filled with dots. At the bottom is a 'Confirm password:' label followed by another password input field filled with dots. At the very bottom are three buttons: 'Cancel', 'Back', and 'Next'.

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

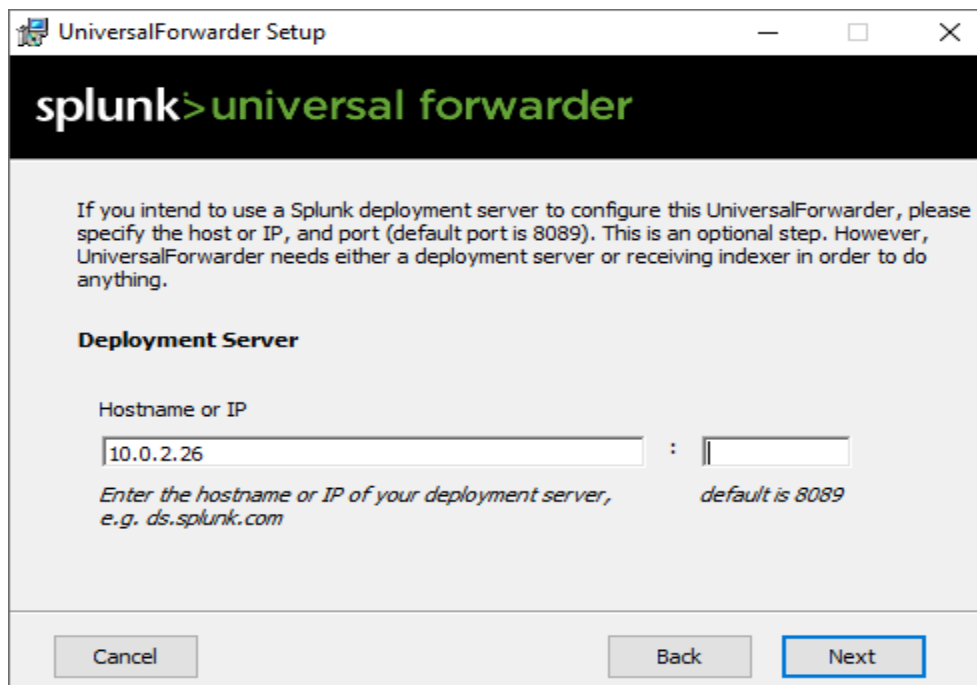
Username:

☐ Generate random password

Password:

Confirm password:

Ahora pondremos la IP de nuestra máquina de Kali Linux, 10.0.2.26. como deployment server, para centralizar la gestión y despliegue de configuraciones, asegurando que todos los datos recolectados se envíen al servidor adecuado para su análisis. El puerto lo dejamos el que viene por defecto .



The screenshot shows the 'UniversalForwarder Setup' window. At the top is the Splunk logo and the text 'universal forwarder'. Below this is an informational paragraph: 'If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.' The section is titled 'Deployment Server'. It contains two input fields: 'Hostname or IP' with the value '10.0.2.26' and a port field with a default value of '8089'. Below the inputs is a note: 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com'. At the bottom are three buttons: 'Cancel', 'Back', and 'Next'.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

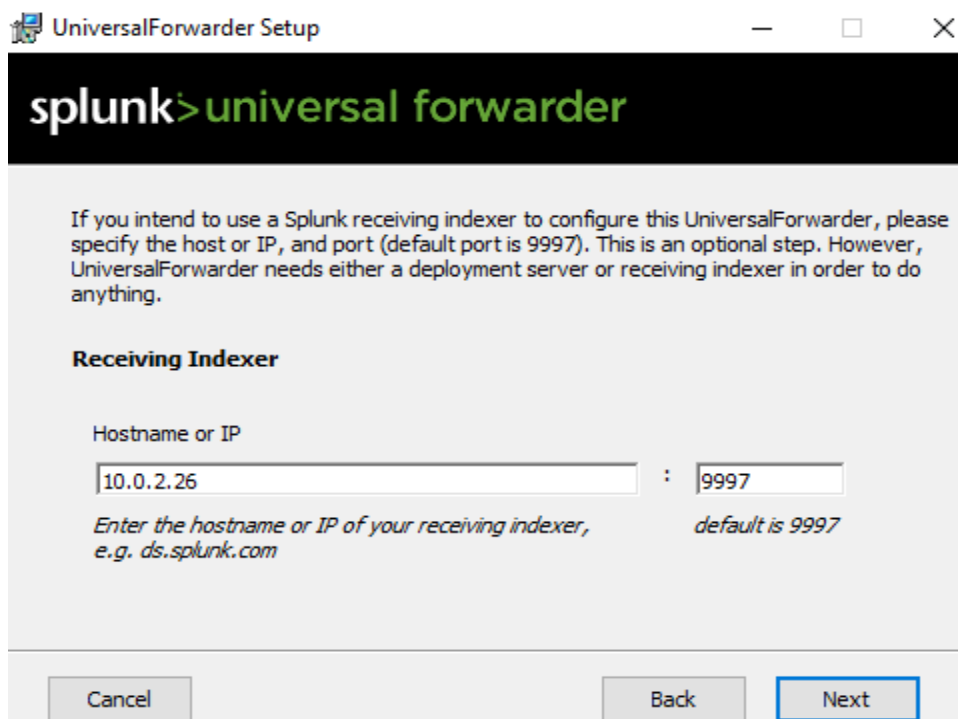
Hostname or IP

10.0.2.26 : 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com default is 8089

Cancel Back Next

En Receiving Indexer volvemos a poner la IP de Kali Linux y puerto 9997.



The screenshot shows the 'UniversalForwarder Setup' window. At the top is the Splunk logo and the text 'universal forwarder'. Below this is an informational paragraph: '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.' The section is titled 'Receiving Indexer'. It contains two input fields: 'Hostname or IP' with the value '10.0.2.26' and a port field with the value '9997'. Below the inputs is a note: 'Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com'. At the bottom are three buttons: 'Cancel', 'Back', and 'Next'.

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

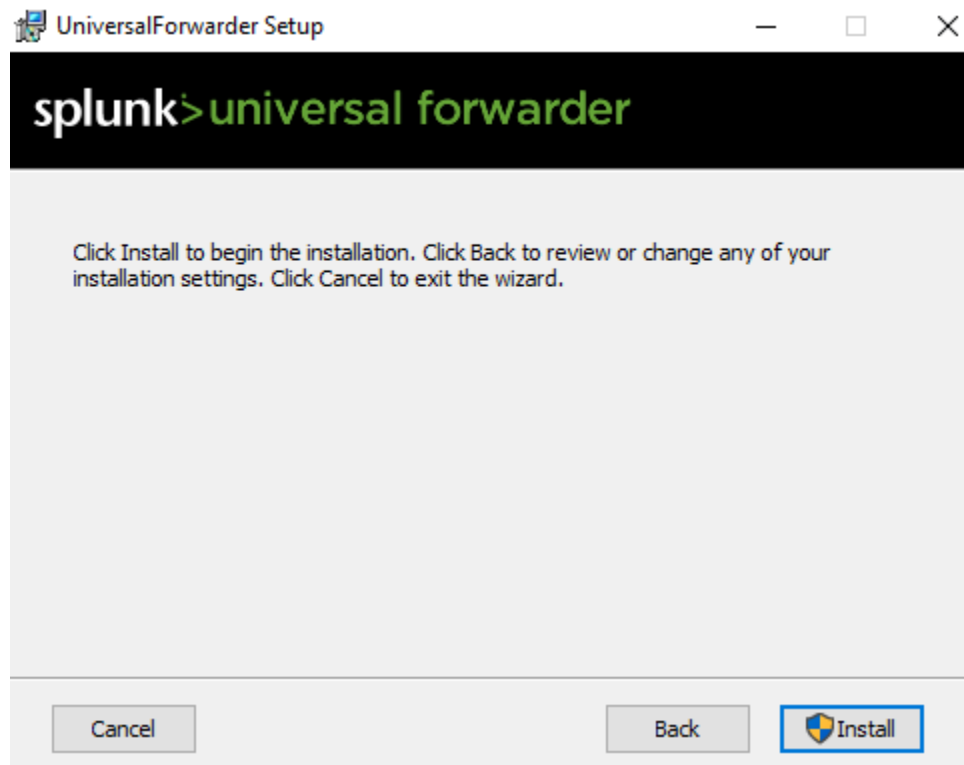
Hostname or IP

10.0.2.26 : 9997

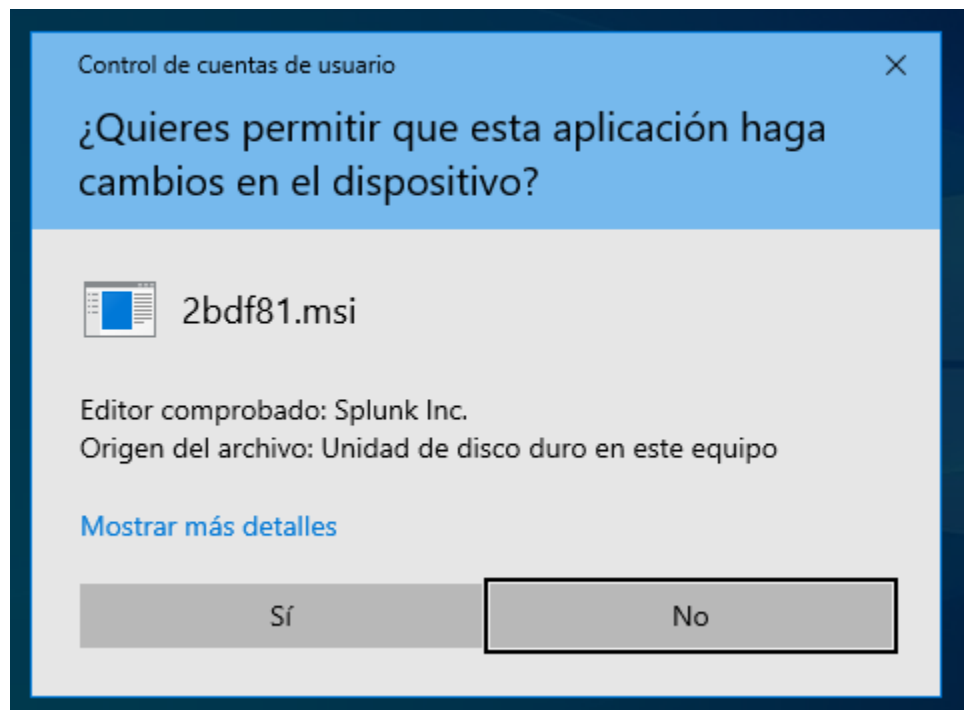
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com default is 9997

Cancel Back Next

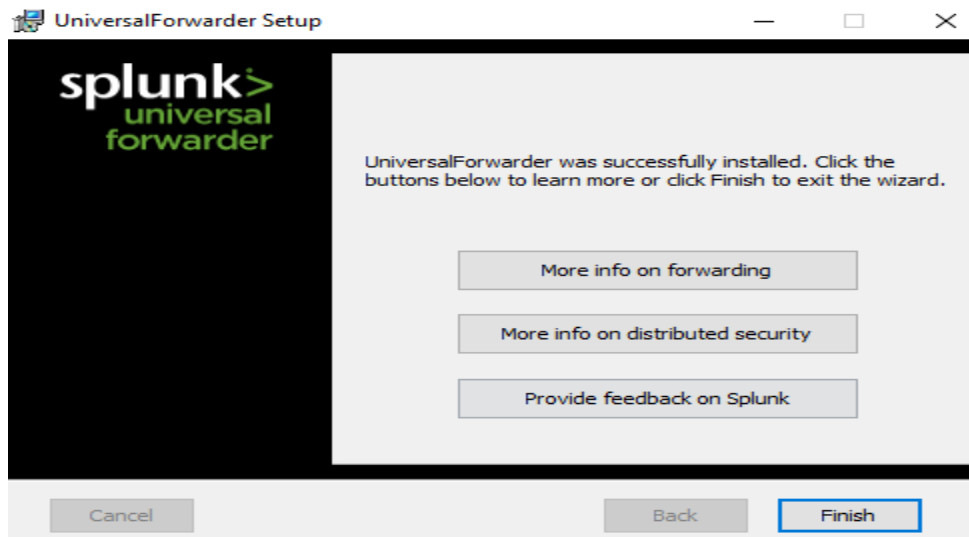
Ahora comenzaremos la instalación.



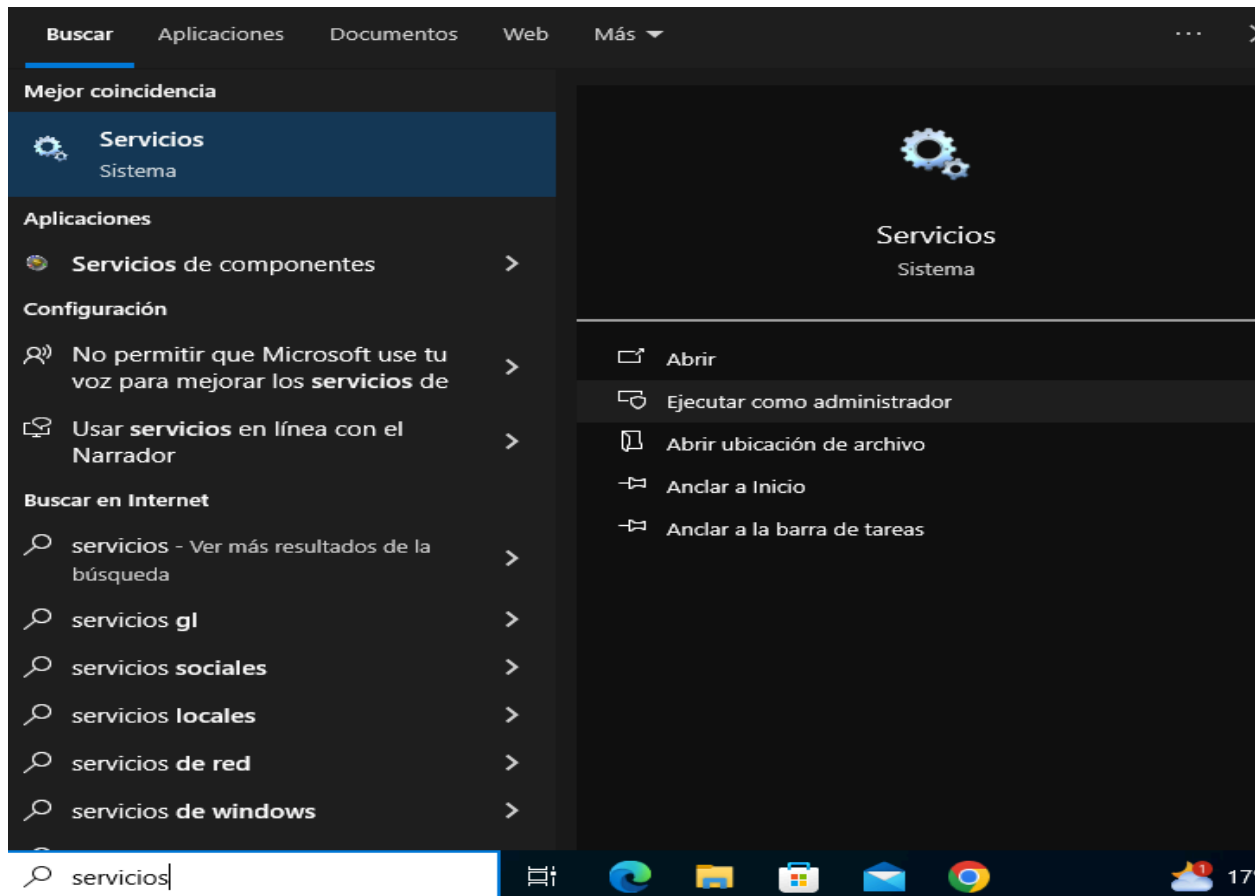
Nos aparecerá una ventana preguntando si autorizamos a esta aplicación a hacer cambios en nuestro ordenador, le diremos que sí.



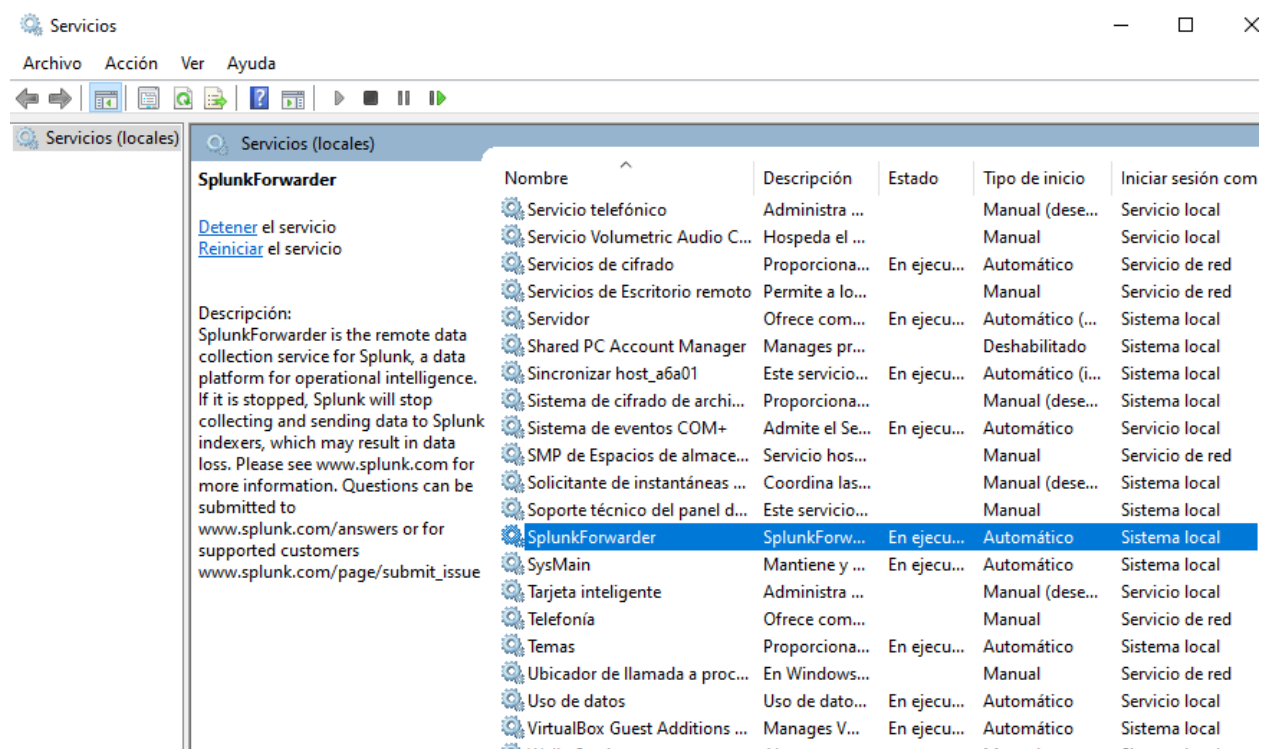
La instalación se realizó exitosamente y le daremos al Finish.



La forma que tenemos para verificar si está correctamente funcionando, es verificar los servicios activos en el ordenador. Para ello, en la barra de búsqueda, buscamos servicios.



Elegimos la opción ejecutar como administrador. Ahora buscaremos SplunkForwarder y veremos que efectivamente está en ejecución.



Ahora vamos a proceder a instalar Sysmon. Para ello, desde nuestra máquina de Windows 10, accedemos a la página web de microsoft sysinternals, en la barra de búsqueda de la izquierda escribimos sysmon y nos encontrará el fichero que queremos descargar.

learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Learn / Sysinternals /

Sysmon v15.14

Article • 02/13/2024 • 10 contributors

[Feedback](#)

In this article

- [Introduction](#)
- [Overview of Sysmon Capabilities](#)
- [Screenshots](#)
- [Usage](#)
- [Show 5 more](#)

By Mark Russinovich and Thomas Garnier

Published: February 13, 2024

[Download Sysmon](#) (4.6 MB)

[Download Sysmon for Linux \(GitHub\)](#)

miércoles, 22 de mayo de 2024

Una vez descargado y descomprimido, podemos ver que nos abrirá la carpeta con este contenido.

Archivo Inicio Compartir Vista

Portapapeles Organizar Nuevo Abrir Selecciones

Este equipo > Descargas > Sysmon

Nombre	Fecha de modificación	Tipo	Tamaño
Eula	13/02/2024 17:03	Documento de te...	8 KB
Sysmon	13/02/2024 17:03	Aplicación	8.250 KB
Sysmon64	13/02/2024 17:03	Aplicación	4.439 KB
Sysmon64a	13/02/2024 17:03	Aplicación	4.883 KB

Abriremos una consola como administrador y nos vamos a la carpeta Downloads/Sysmon, y ejecutamos el siguiente comando:

```
sysmon64 -i -n -h md5 -accepteula
```

```
C:\Users\Admin\Downloads\Sysmon>sysmon64 -i -n -h md5 -accepteula

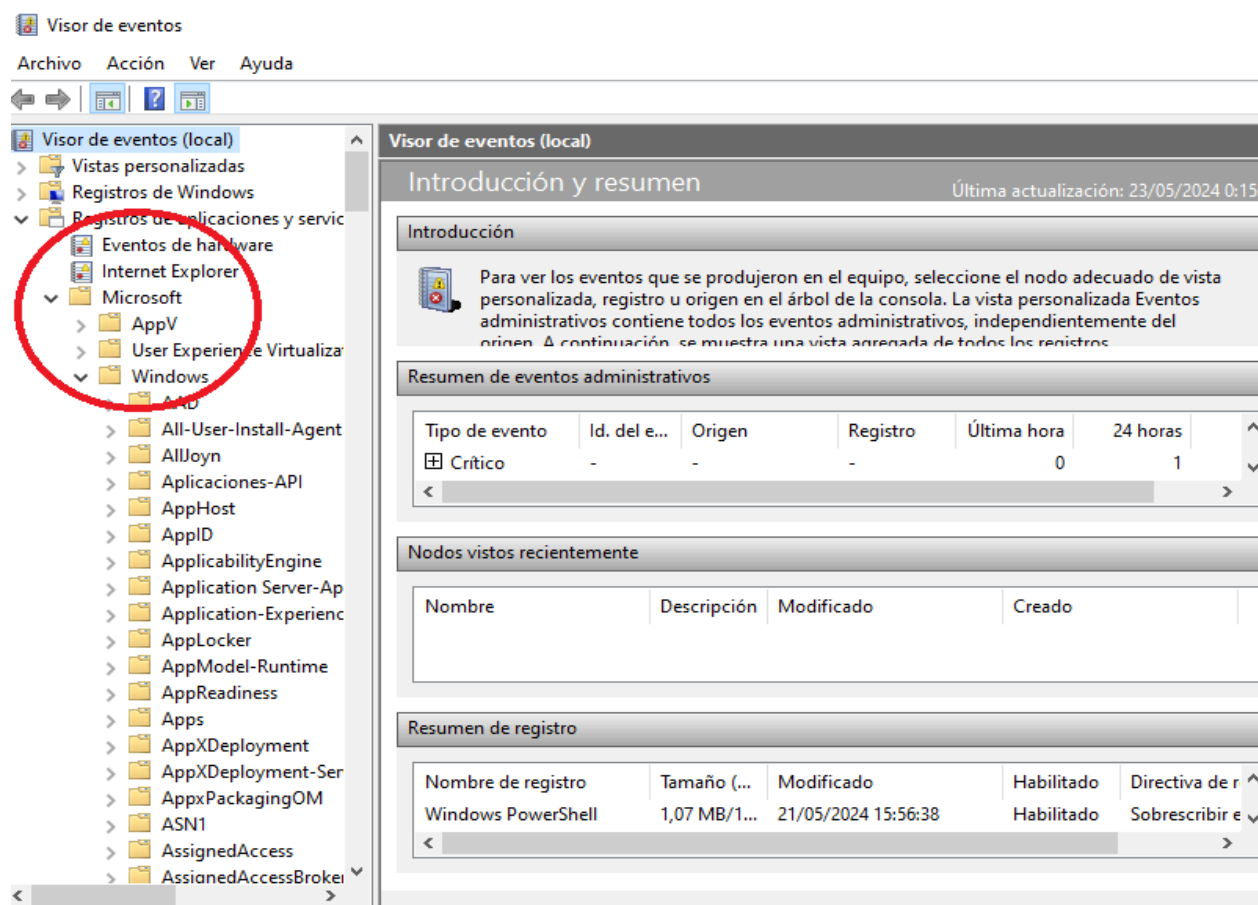
System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\Admin\Downloads\Sysmon>
```

Verificamos que se instaló correctamente y que está activo.

Ahora tenemos que verificar que Sysmon está funcionando y generando eventos en el visor de eventos de Windows, para ello abriremos el visor de eventos.



Tenemos que bajar hasta encontrar Sysmon y dentro de la carpeta Sysmon, hay un fichero Operational, que es donde se guardan todos los logs generados

Operational Número de eventos: 181

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	23/05/2024 0:17:56	Sysmon	3	Network co...
Información	23/05/2024 0:17:55	Sysmon	3	Network co...
Información	23/05/2024 0:17:55	Sysmon	3	Network co...
Información	23/05/2024 0:17:55	Sysmon	3	Network co...
Información	23/05/2024 0:17:54	Sysmon	3	Network co...
Información	23/05/2024 0:17:54	Sysmon	3	Network co...
Información	23/05/2024 0:17:52	Sysmon	3	Network co...
Información	23/05/2024 0:17:52	Sysmon	3	Network co...
Información	23/05/2024 0:17:47	Sysmon	3	Network co...
Información	23/05/2024 0:17:09	Sysmon	3	Network co...
Información	23/05/2024 0:17:09	Sysmon	3	Network co...
Información	23/05/2024 0:17:09	Sysmon	3	Network co...
Información	23/05/2024 0:16:39	Sysmon	3	Network co...
Información	23/05/2024 0:16:39	Sysmon	3	Network co...

Evento 3, Sysmon

General Detalles

Network connection detected:
RuleName: ...

Nombre de registro: Microsoft-Windows-Sysmon/Operational
Origen: Sysmon Registrado: 23/05/2024 0:17:56
Id. del: 3 Categoría de tarea: Network connection deter

Si miramos el último log generado, podemos ver que fue cuando activamos el servicio Sysmon, podemos ver el comando ejecutado cuando entramos en la pestaña detalles.

Operational Número de eventos: 181 (!) Nuevos eventos disponibles

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	23/05/2024 0:10:42	Sysmon	3	Network co...
Información	23/05/2024 0:10:42	Sysmon	3	Network co...
Información	23/05/2024 0:10:13	Sysmon	1	Process Cre...
Información	23/05/2024 0:10:12	Sysmon	5	Process ter...
Información	23/05/2024 0:10:11	Sysmon	1	Process Cre...
Información	23/05/2024 0:10:11	Sysmon	1	Process Cre...
Información	23/05/2024 0:10:11	Sysmon	4	Sysmon serv...
Información	23/05/2024 0:10:11	Sysmon	16	Sysmon con...

Evento 16, Sysmon









General Detalles

☒ Vista descriptiva ☐ Vista XML

+ System
- EventData
 UtcTime 2024-05-22 22:10:11.331
 Configuration C:\Users\Admin\Downloads\Sysmon\sysmon64
 -i -n -h md5 -accepteula
 ConfigurationFileHash -

Podemos observar que nos dá información de usuario, hora, categoría, origen,etc.

Operational Número de eventos: 181 (!) Nuevos eventos disponibles

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
 Información	23/05/2024 0:10:42	Sysmon	3	Network co...
 Información	23/05/2024 0:10:42	Sysmon	3	Network co...
 Información	23/05/2024 0:10:13	Sysmon	1	Process Cre...
 Información	23/05/2024 0:10:12	Sysmon	5	Process ter...
 Información	23/05/2024 0:10:11	Sysmon	1	Process Cre...
 Información	23/05/2024 0:10:11	Sysmon	1	Process Cre...
 Información	23/05/2024 0:10:11	Sysmon	4	Sysmon serv...
 Información	23/05/2024 0:10:11	Sysmon	16	Sysmon con...

Evento 16, Sysmon

General Detalles

Sysmon config state changed:
UtcTime: 2024-05-22 22:10:11.331

Nombre de registro: Microsoft-Windows-Sysmon/Operational

Origen: Sysmon

Registrado: 23/05/2024 0:10:11

Id. del 16

Categoría de tarea: Sysmon config state change

Nivel: Información

Palabras clave:

Usuario: W10\Admin

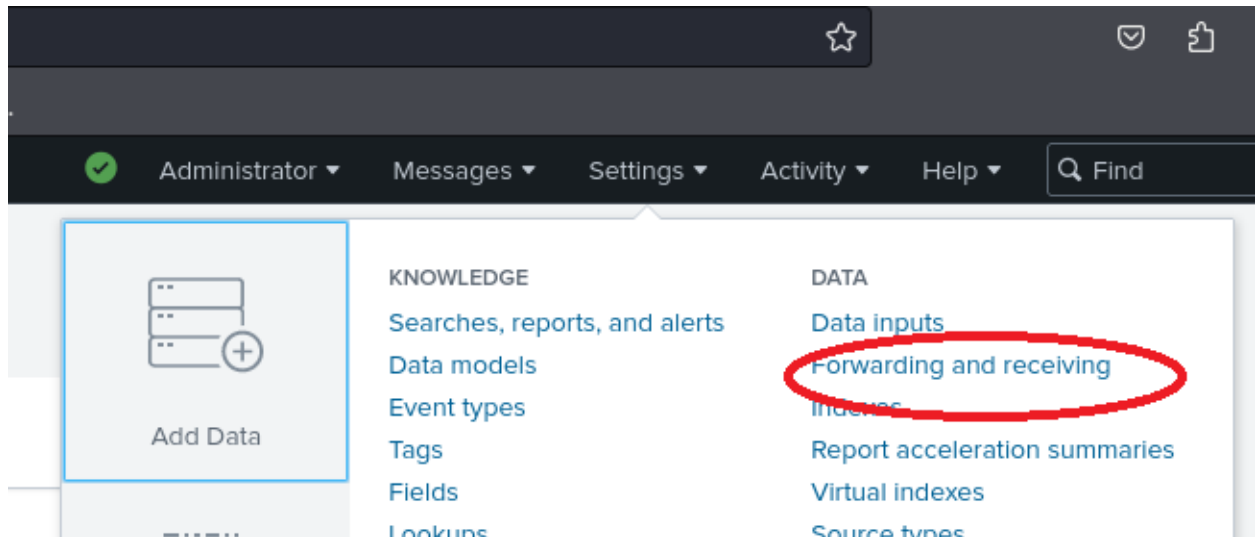
Equipo: W10.bosquempresa.local

Código de operación: Información

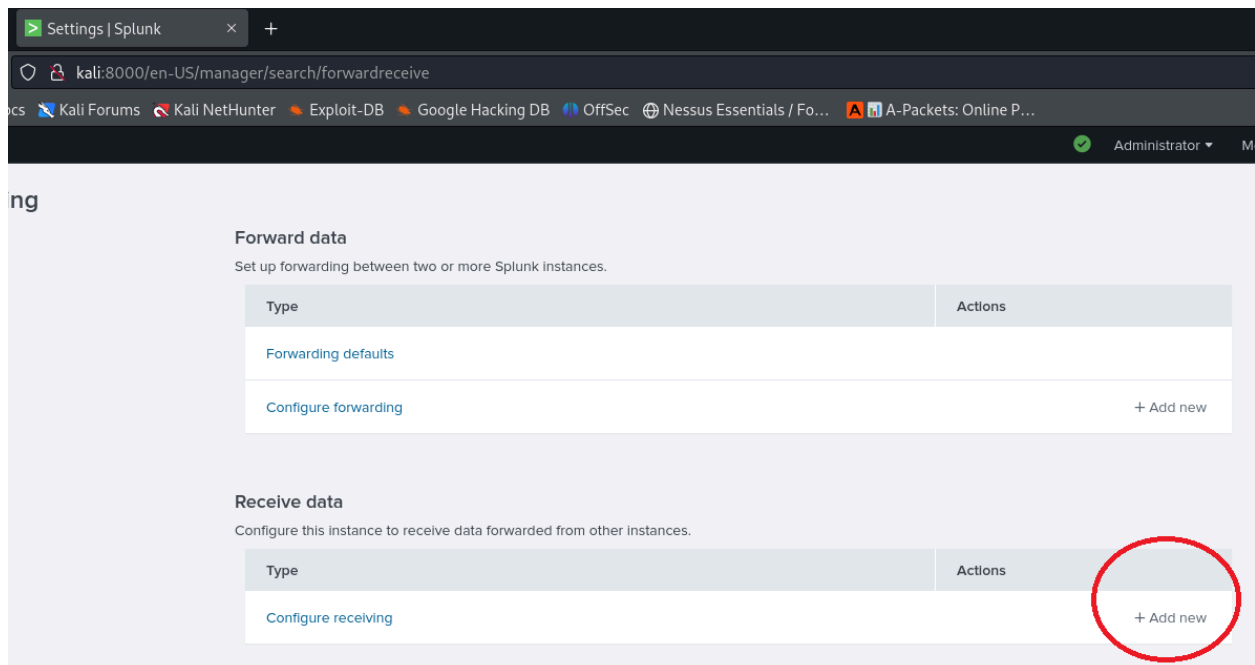
Más información: [Ayuda Registro de eventos](#)

Configuración de Splunk para Recibir Eventos de Sysmon

El siguiente paso ahora será ir a Kali Linux, abrir el navegador, ir al dashboard principal de Splunk > Settings > Add Data > Forwarding



Una vez dentro de esta pestaña, iremos a add new, dentro de Receiving Data.



Configuramos el puerto 9997 para que quede a la escucha y guardamos.

Configure receiving

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

Listen on this port *

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

Cancel

Save

Forwarding and receiving > receive data

Successfully saved "9997".

Showing 1-1 of 1 item

filter

Listen on this port ▾	Status ▾	Actions
9997	Enabled Disable	Delete

Podemos verificar que está correctamente a la escucha.

```
(root@kali)-[/opt/splunk/bin]
# lsof -i:9997
COMMAND    PID  USER   FD   TYPE    DEVICE  SIZE/OFF  NODE  NAME
splunkd    210572 root    181u  IPv4    784135      0t0   TCP  *:9997 (LISTEN)
```

Configuración de Data Inputs

Los Data Inputs son diversas fuentes desde las cuales Splunk puede recolectar datos, incluyendo archivos de registro (logs), flujos de red, eventos de Windows, métricas, y datos de API, permitiendo una ingesta y análisis centralizado de información en tiempo real. Para configurar esto, debemos ir nuevamente al dashboard de Splunk > Settings > Add Data > Data Inputs.

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	18	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	25	+ Add new
Splunk Assist Instance Identifier Assigns a random identifier to every node	1	+ Add new
Systemd Journal Input for Splunk This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
Logd Input for the Splunk platform	0	+ Add new

Buscamos Forwarded Inputs y agregamos uno de Windows Event Logs.

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	+ Add new

Le pondremos Windows como nombre de New Server Class y seleccionamos add all.

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn](#)

! At least one forwarding host must be selected.

Select Server Class

New

Existing

Available host(s)

[add all »](#)

WINDOWS W10

Selected host(s)

[« remove all](#)

WINDOWS W10

New Server Class Name

Windows

Volvemos a seleccionar todas las opciones.

Add Data

Select Forwarders

Select Source

Input Settings

Review

Done

< Back

Next >

I file, or monitor an entire directory.

form to listen on a network port.

evice, or database with a script.

Identifier

er to every node

ut for Splunk

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs

Available item(s)

add all »

Application

ForwardedEvents

Security

Setup

System

Selected item(s)

Application

ForwardedEvents

Security

Setup

System

Select the Windows Event Logs you want to index from the list.

Dejamos Input Settings como viene por defecto.

The screenshot shows the 'Input Settings' step of the 'Add Data' wizard. At the top, a progress bar indicates the sequence: Select Forwarders, Select Source, Input Settings (current), Review, and Done. The 'Input Settings' section has a title and a description: 'Optionally set additional input parameters for this data input as follows:'. Below this, the 'Index' setting is shown with a dropdown menu set to 'Default' and a link to 'Create a new index'. A 'Learn More' link is also present.

Add Data

Select Forwarders Select Source **Input Settings** Review Done

Input Settings

Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default [Create a new index](#)

Verificamos que está todo correcto y le damos a submit.

The screenshot shows the 'Review' step of the 'Add Data' wizard. The progress bar at the top shows the sequence: Select Forwarders, Select Source, Input Settings, Review (current), and Done. The 'Review' section displays the configuration details for the data input: Server Class Name (Windows), List of Forwarders (WINDOWS | W10), Collection Name (localhost), Input Type (Windows Event Logs), Event Logs (Application, ForwardedEvents, Security, Setup, System), and Index (default). A 'Submit' button is visible at the top right.

Add Data

Select Forwarders Select Source Input Settings **Review** Done

Review

Server Class Name Windows

List of Forwarders WINDOWS | W10

Collection Name localhost

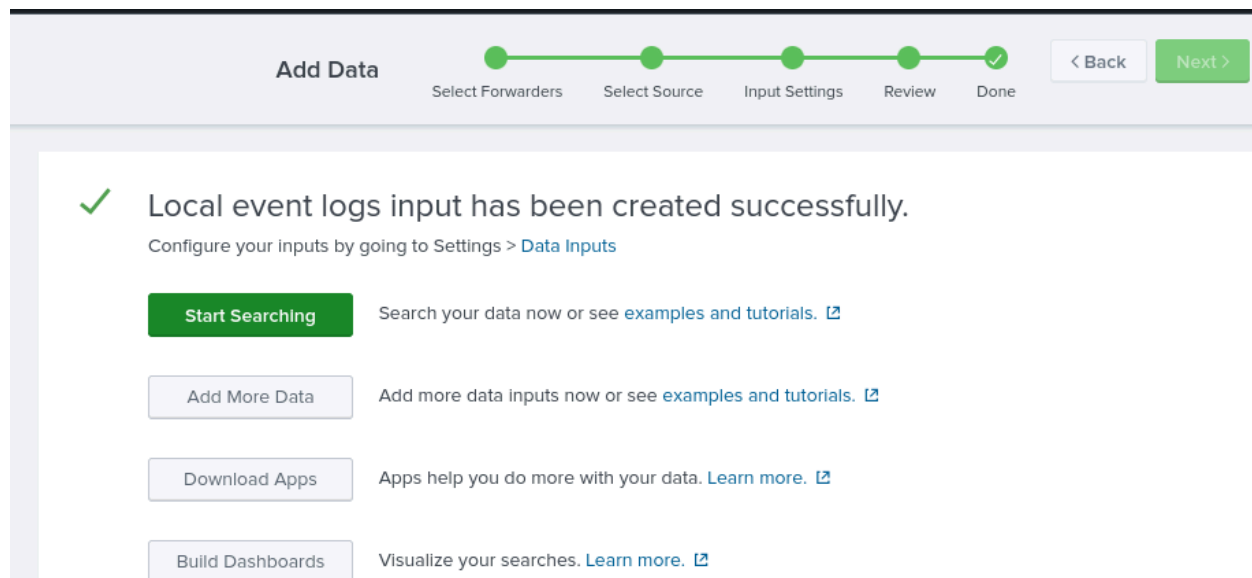
Input Type Windows Event Logs

Event Logs Application
ForwardedEvents
Security
Setup
System

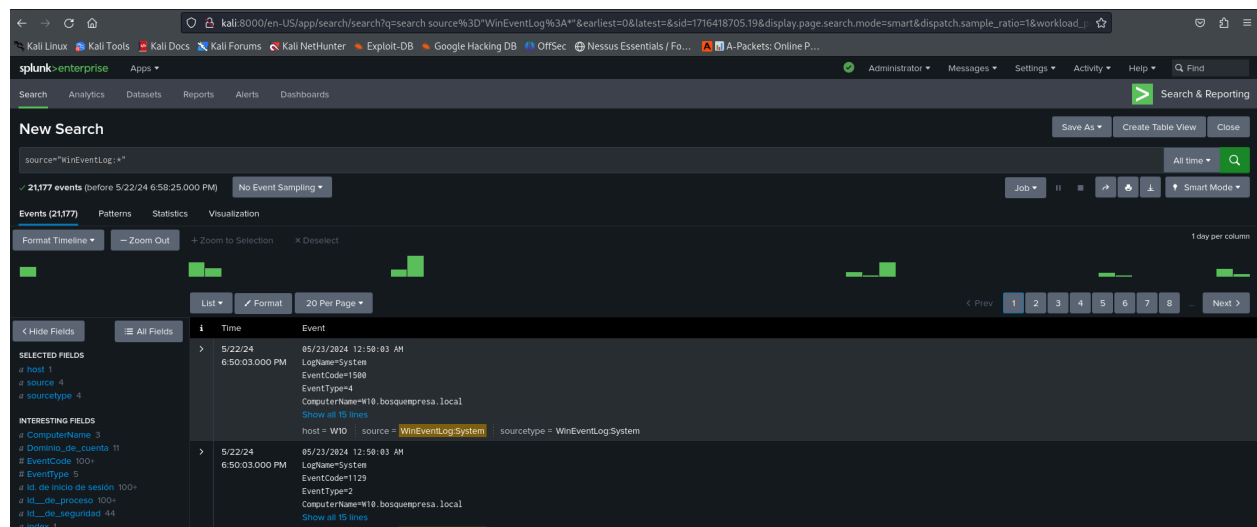
Index default

[Back](#) **Submit**

Verificamos que se crearon correctamente.



Ahora empezaremos a buscar los logs de eventos locales, para ello le daremos a Start Searching y nos abrirá todos los eventos creados en nuestro Dashboard. Se verá de esta forma.



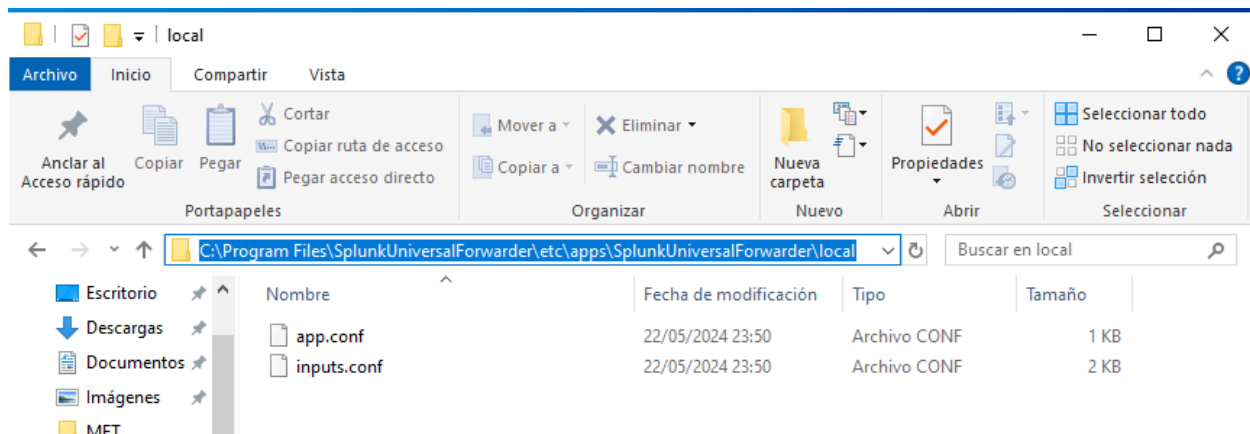
Una vez cargados los data inputs en Splunk, podemos usar varios parámetros para buscar y filtrar datos, como:

1. Keywords: Palabras clave específicas dentro de los eventos.
2. Time Range: Especificar intervalos de tiempo.
3. Fields: Filtrar por campos específicos (e.g., host, source, sourcetype).
4. Boolean Operators: Utilizar AND, OR, NOT para combinar condiciones.

5. Wildcards: Usar * para búsquedas de patrones.
6. Pipes: (|) Para encadenar comandos y refinar resultados.
7. Comparison Operators: Filtrar usando =, !=, <, >, <=, >=.

Ejemplo de búsqueda: `sourcetype="access_combined" status=200 | stats count by host`.

Pudimos verificar que funciona correctamente, lo que haremos ahora será modificar el fichero `inputs.conf` en la máquina de Windows 10. Para ello iremos a la carpeta `C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local`.



Allí abriremos el fichero con bloc de notas y le agregaremos las siguientes líneas:

```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
```

```
checkpointInterval = 5
```

```
current_only = 0
```

```
disabled = 0
```

```
start_from = oldest
```

```

*inputs: Bloc de notas
Archivo Edición Formato Ver Ayuda
[WinEventLog://ForwardedEvents]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventLog://Setup]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

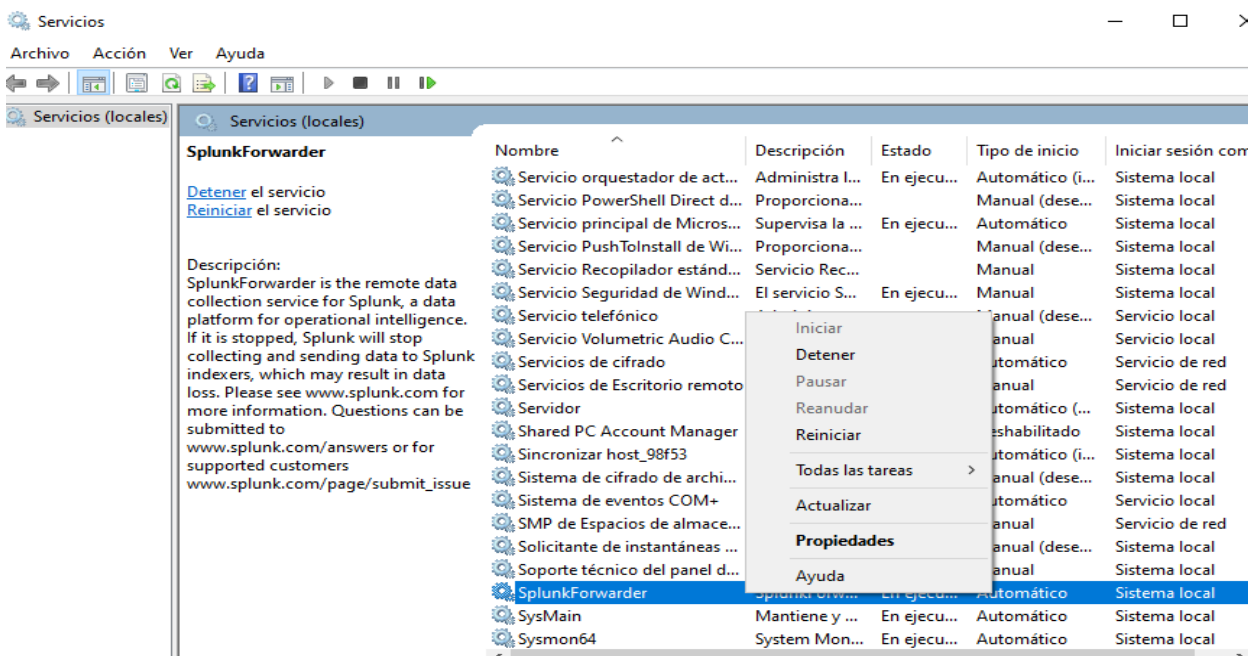
[admon://NearestDC]
monitorSubtree = 1

[perfmon://CPU Load]
counters = % Processor Time;% User Time
instances = Total

```

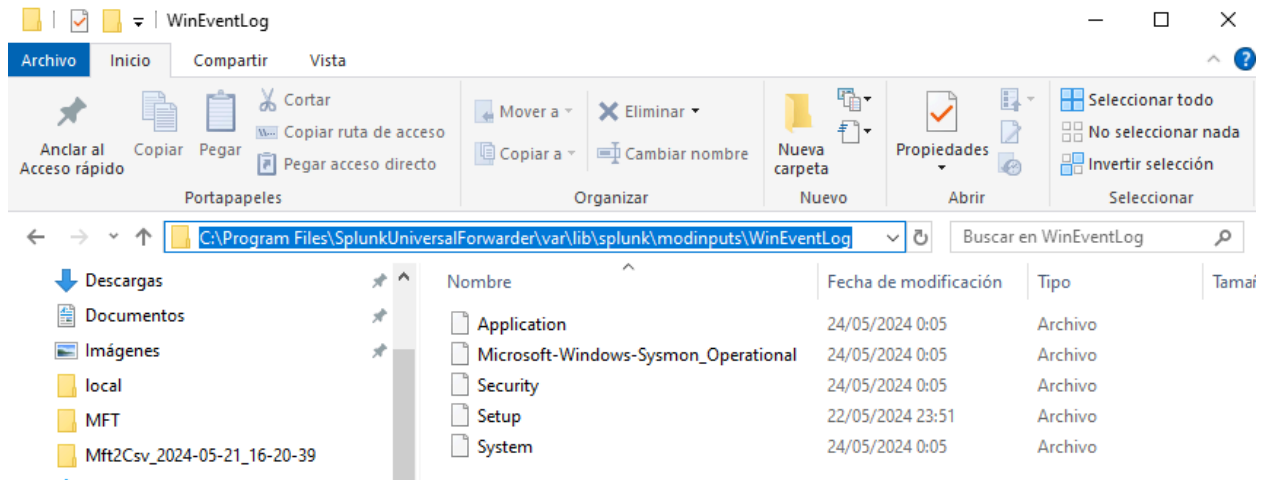
Debemos cambiar permisos para que nos deje modificar este fichero.

Ahora iremos a Servicios nuevamente y sobre Splunk Forwarder, daremos a actualizar.



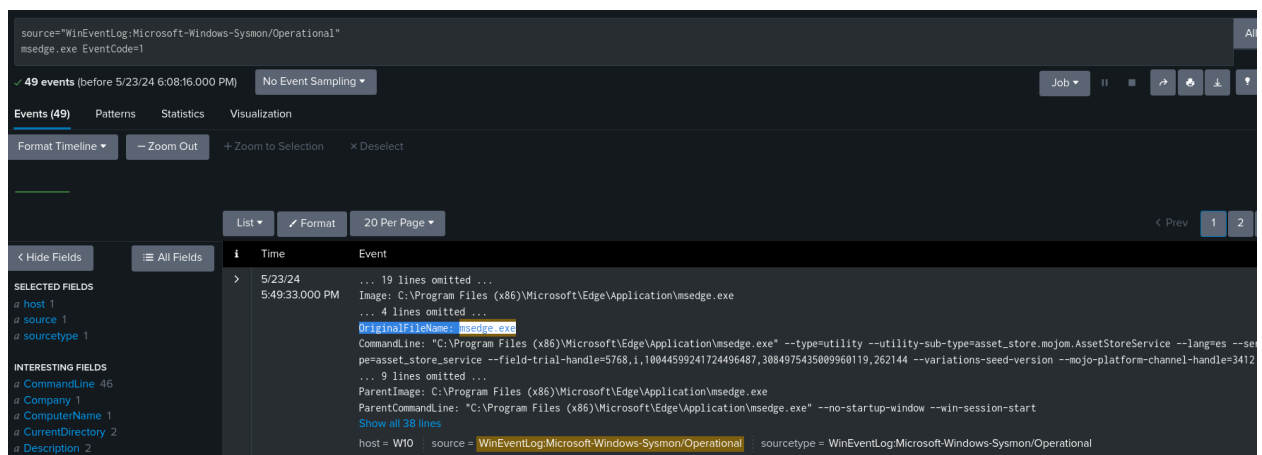
Si vamos a la carpeta:

C:\ProgramFiles\SplunkUniversalForwarder\var\lib\splunk\modinputs\WinEventLog
veremos un fichero nuevo creado con el nombre
Microsoft-Windows-Sysmon-Operational.



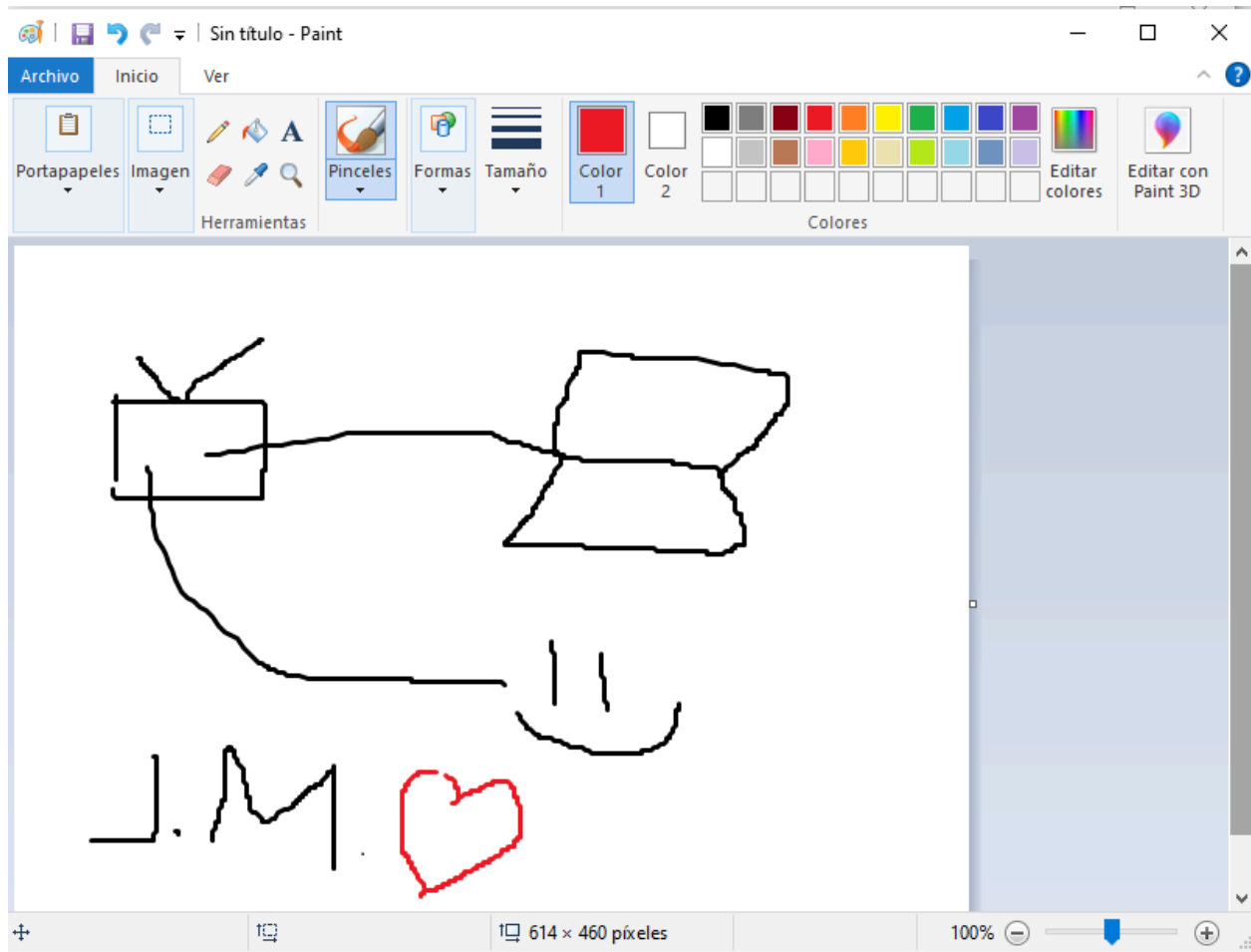
Para verificar que Splunk está recibiendo correctamente los eventos de sysmon, nos iremos a nuestra máquina de Kali Linux y en el Dashboard, en la barra de búsqueda, buscaremos el siguiente parámetro:

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational"msedge.exe  
EventCode=1
```



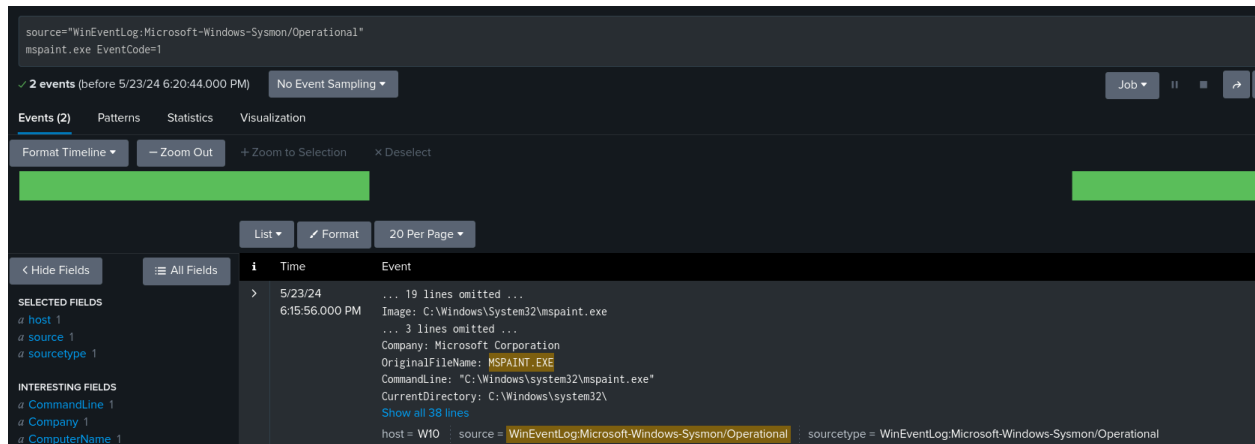
Generación de Eventos de Seguridad

Ahora lo que haremos será crear distintos “movimientos” dentro de la máquina de Windows 10, para generar logs y poder captarlos desde Splunk en Kali Linux. Primero probaremos abriendo un paint y haciendo un dibujo y guardarlo en el escritorio.

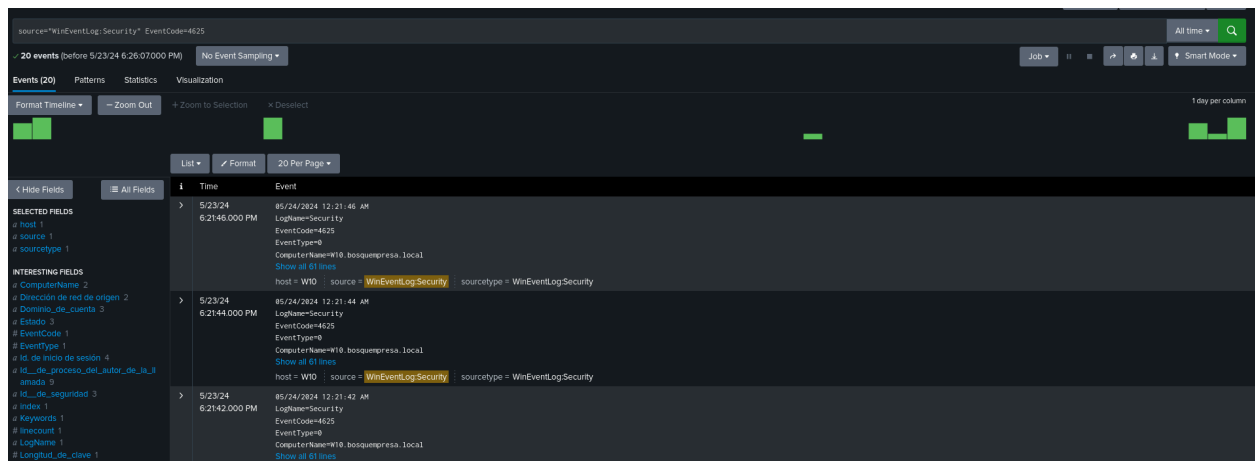


Ahora vamos a la máquina de Kali Linux y usamos el siguiente parámetro de búsqueda:

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational"mspaint.exe  
EventCode=1
```



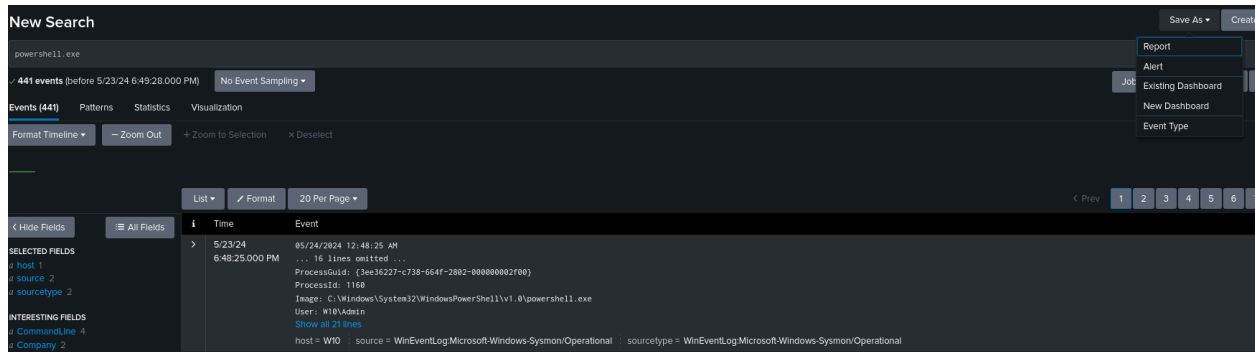
Ahora vamos a probar con otro tipo de evento, intentos de login incorrectos.



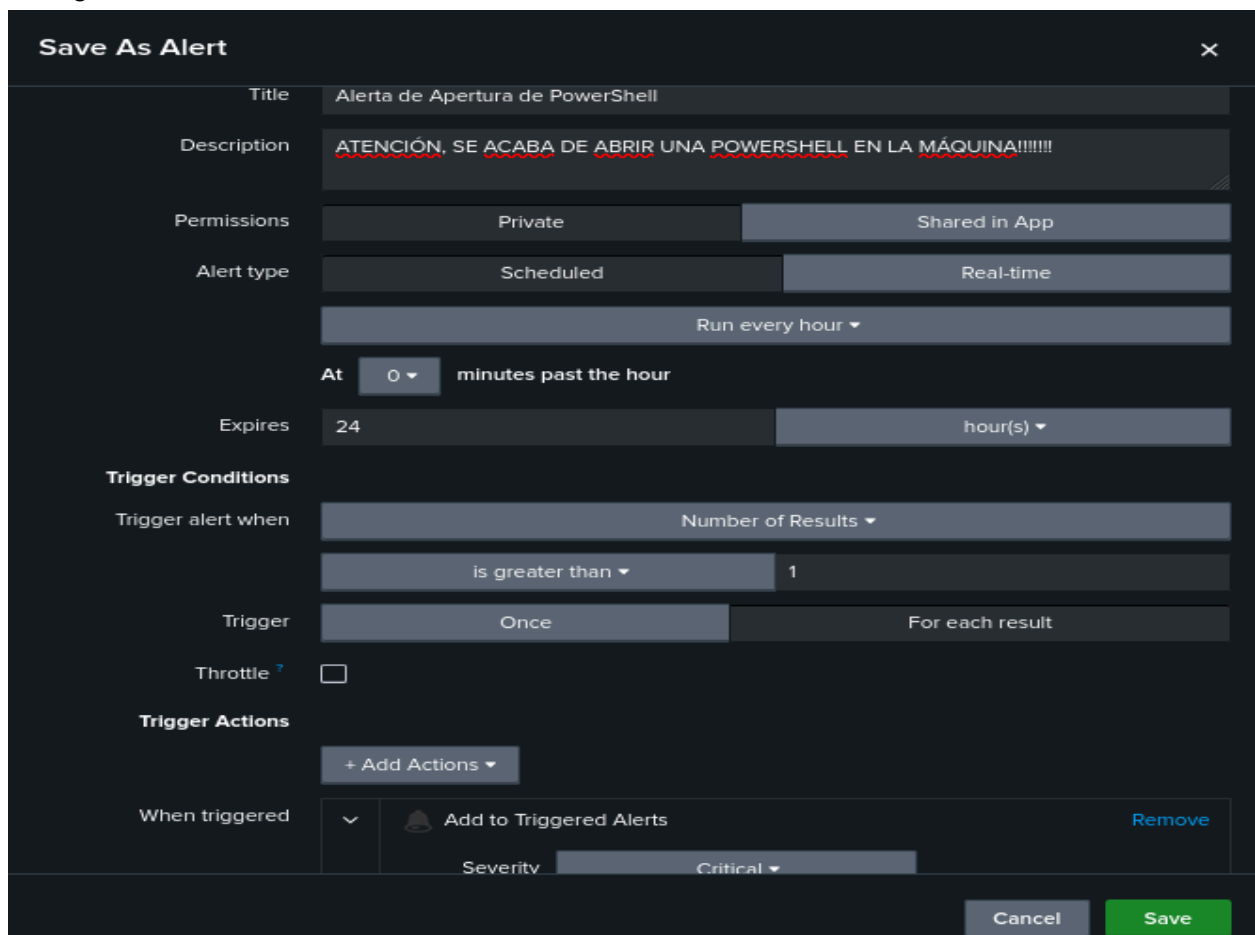
De esta manera, sin querer probamos más de 3 veces y se bloqueó la cuenta. Apagamos el ordenador y esperamos un rato y se vuelve a desbloquear.

Análisis de Eventos en Splunk

En este último punto del ejercicio, debemos crear búsquedas y alertas, para ello iremos al dashboard de Splunk en nuestra máquina de Kali Linux. Ahora vamos a generar un alerta para que en el caso de que se abra powershell en la máquina de Windows 10, nos avise. Primero en la barra de búsqueda escribiremos powershell.exe. Una vez encontramos el log que generamos (anteriormente debemos ir a windows 10 y ejecutar una powershell), iremos a la pestaña Save as > Alert.



Configuramos la alerta:



Save As Alert

Title: Alerta de Apertura de PowerShell

Description: ATENCIÓN, SE ACABA DE ABRIR UNA POWERSHELL EN LA MÁQUINA!!!!!!

Permissions: Private

Alert type: Scheduled

Run every hour

At 0 minutes past the hour

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results is greater than 1

Trigger: Once

Throttle: ☐

Trigger Actions

+ Add Actions

When triggered: Add to Triggered Alerts

Severity: Critical

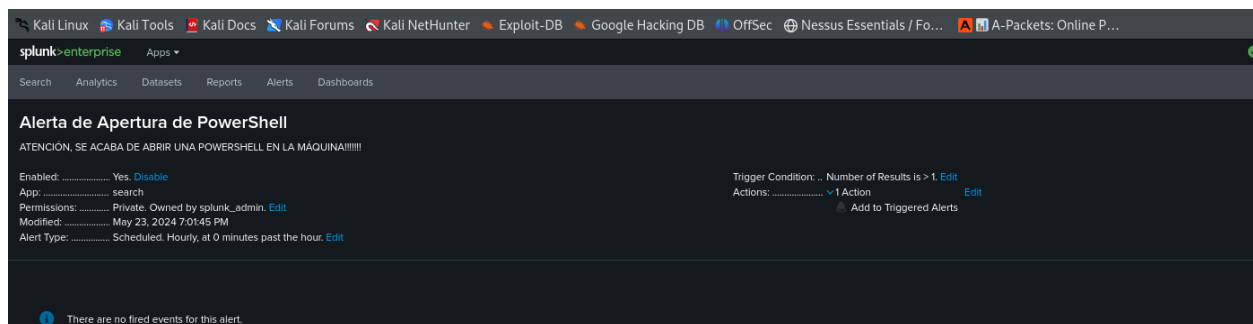
Cancel Save

Le pondremos un nombre a la alerta, una descripción, le pondremos que sea cada hora, que el número de resultados sea a partir de 1 y que aparezca esta alerta cada vez que se ejecute la powershell.

"Triggered alerts" (alertas activadas) se refiere a alertas que se activan o desencadenan en un sistema de monitoreo o análisis cuando se cumple cierta condición o criterio predefinido. Estas alertas son generadas automáticamente por el sistema y pueden ser configuradas para notificar a los usuarios o administradores sobre eventos importantes o anomalías que requieran atención inmediata.

Por ejemplo, en Splunk, una alerta activada podría configurarse para detectar un aumento repentino en el número de intentos de acceso fallidos a un sistema, lo que podría indicar un intento de intrusión. Cuando se activa esta alerta, Splunk puede enviar una notificación por correo electrónico o ejecutar una acción específica, como bloquear la dirección IP del atacante o generar un ticket en un sistema de seguimiento de problemas.

Podemos ver la alerta configurada correctamente.



Conclusiones

Este ejercicio nos proporcionó una experiencia práctica sobre la implementación y configuración de herramientas fundamentales para el monitoreo de seguridad y el análisis de eventos. A través de la instalación y configuración de Splunk y Sysmon, así como la generación y análisis de eventos de seguridad, se obtuvieron una serie de conclusiones importantes:

1. **Implementación Efectiva de Splunk y Sysmon:** La instalación y configuración exitosa de Splunk y Sysmon demostraron ser fundamentales para establecer un entorno de monitoreo de seguridad local efectivo. La capacidad de Splunk para recibir, indexar y analizar eventos de Sysmon permitió una visibilidad mejorada de la actividad del sistema y la detección temprana de posibles amenazas.
2. **Configuración de Alertas para la Detección de Eventos Críticos:** La configuración de alertas en Splunk permitió la detección automática de eventos críticos de seguridad, como la apertura de PowerShell, proporcionando una capa adicional de defensa contra posibles amenazas. Estas alertas permitieron una respuesta proactiva a eventos de seguridad importantes, mejorando así la postura de seguridad general del entorno.
3. **Documentación Detallada:** La documentación detallada de cada paso realizado durante el ejercicio proporcionó un recurso valioso para futuras referencias y aprendizaje en el campo de la ciberseguridad y el análisis de logs. La práctica reforzó la importancia de mantener registros precisos y detallados de las configuraciones y acciones realizadas en entornos de seguridad.
4. **Alertas Activadas como Herramienta fundamental de Seguridad:** La configuración y utilización de alertas activadas en Splunk destacó su importancia como una herramienta fundamental en la detección temprana y la respuesta a incidentes de seguridad. La capacidad de configurar alertas para eventos específicos permitió una respuesta rápida y efectiva a posibles amenazas, ayudando a mitigar el impacto de los incidentes de seguridad.