

Actividad 3 - Splunk

Módulo 3: Gestión de incidentes

Diego Mucci

21/05/2024

Seguridad Informática

Actividad 3 - Splunk

Splunk es una plataforma avanzada de software diseñada para buscar, monitorizar y analizar datos generados por máquinas en tiempo real. Se especializa en gestionar grandes volúmenes de datos provenientes de diversas fuentes, como registros de aplicaciones, sistemas, dispositivos de red y sensores IoT. Utiliza un lenguaje de búsqueda propio llamado SPL (Search Processing Language) que permite a los usuarios extraer información valiosa y visualizarla mediante gráficos, tablas y dashboards personalizados.

El propósito principal de Splunk es ayudar a las organizaciones a convertir datos complejos y desestructurados en información accionable. Facilita la detección de problemas de rendimiento, la supervisión de seguridad, la auditoría de cumplimiento y la obtención de insights operacionales. Al permitir una visión completa y en tiempo real de la infraestructura tecnológica, Splunk es una herramienta esencial para administradores de sistemas, analistas de seguridad y profesionales de TI en general, mejorando la eficiencia operativa y la capacidad de respuesta ante incidentes.

Splunk no es exclusivamente un SIEM (Security Information and Event Management), pero sí puede funcionar como tal. Originalmente, Splunk fue desarrollado como una plataforma de búsqueda y análisis de datos generados por máquinas, enfocándose en la gestión de grandes volúmenes de datos y la obtención de información operativa a partir de ellos.

Sin embargo, Splunk ha ampliado su funcionalidad y, con aplicaciones y módulos específicos, puede ser utilizado como un SIEM. Al integrar capacidades de recopilación, análisis y correlación de eventos de seguridad en tiempo real, Splunk permite a las organizaciones detectar, investigar y responder a amenazas de seguridad de manera eficaz. Esto lo convierte en una herramienta muy versátil que, con las configuraciones y complementos adecuados, puede cumplir con las funciones de un SIEM tradicional, ofreciendo una visión integral de la seguridad y el cumplimiento normativo dentro de una infraestructura tecnológica.

Actividad: Implementación de Splunk en Entorno Local

Objetivo:

Los alumnos instalarán Splunk en un entorno local, desplegarán Sysmon en una máquina virtual Windows, y configurarán Splunk para recibir y analizar eventos de seguridad. Documentarán el proceso con capturas de pantalla y generarán eventos de seguridad para verificar la correcta configuración y funcionamiento.

Requisitos:

- Acceso a una máquina virtual o física para instalar Splunk (Virtual-Kali)

- Acceso a una máquina virtual Windows para instalar Sysmon
- Cuenta en Splunk para descargar el software
- Acceso a internet para descargar instaladores y actualizaciones

Pasos a seguir:

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.

1. Instalación de Splunk en Entorno Local

Nos descargamos el programa desde la página oficial, pero primero para ello nos deberemos registrar:

The screenshot shows the Splunk Enterprise download page. The top navigation bar includes links for Products, Solutions, Why Splunk?, Resources, Company, and Support. The main heading is "Splunk Enterprise" with a subheading "Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required." Below this is a "Get My Free Trial" button. The page then transitions to a registration form titled "Start Your Free Download". The form includes fields for Business Email, Password, First Name, Last Name, Job Title, and Phone Number. A "Log in" link is provided for existing users. The form is set against a background of colorful geometric shapes.

Después de esto, se nos enviará un correo de verificación. Una vez verificada la cuenta podemos optar por descargamos la instalación para Windows, Linux o Mac OS.

The screenshot shows the Splunk Enterprise 9.2.1 download page. The page is titled "Splunk Enterprise 9.2.1" and includes a subheading "Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments." Below this is a "Choose Your Installation Package" section. The page is divided into three tabs: Windows, Linux, and Mac OS. The Linux tab is currently selected. Under the Linux tab, there are three rows of installation packages: 64-bit Windows 10 Windows Server 2019, 2022 (509.24 MB), 3.x+, 4.x+, or 5.4.x kernel Linux distributions (520.37 MB), and 679.42 MB (679.24 MB). Each row has a "Download Now" button and a "Copy wget link" button. The page also includes links for Release Notes, System Requirements, Previous Releases, and All Other Downloads.

Nos descargaremos la versión tanto para Windows como para Linux. Para Linux seleccionaremos la opción Linux.deb que es compatible con nuestro Kali Linux.

En nuestro Kali Linux, nos dirigimos a la carpeta *Downloads*, para observar que se haya descargado correctamente el archivo e instalamos Splunk ejecutando el comando “dpkg -i + nombre del archivo”:

```
(root@kali)~/home/kali/Downloads
# ls
ZAP_2_14_0_unix.sh  coreruleset  snort3-libdaq-v3.0.14-0-gae68d7b.tar.gz  snort3-snort3-3.1.04.0-0-g07312ef.tar.gz  snort3-snort3_extra-3.1.03.0-0-gb01a2e4.tar.gz  snort_user.pdf  splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb

(root@kali)~/home/kali/Downloads
# dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 394394 files and directories currently installed.)
Preparing to unpack splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
```

Después, vamos al directorio */opt/splunk* creado recientemente y accedemos a la carpeta *bin* para ver si todos los archivos han sido instalados correctamente:

```
(root@kali)~/home/kali/Downloads
# cd /opt/splunk

(root@kali)~/opt/splunk
# dir
README-splunk.txt  bin  cmake  copyright.txt  etc  ftr  include  lib  license-eula.txt  openssl  opt  quarantined_files  share  splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest  swidtag

(root@kali)~/opt/splunk
# cd bin

(root@kali)~/opt/splunk/bin
# ls
2to3-3.7  classify  genRootCA.sh  jars  noah_self_storage_archiver.py  prichunkpng  pydoc3.7  rest_handler.py  slim
ColdStorageArchiver.py  coldToFrozenExample.py  genSignedServerCert.py  jsmin  node  priforgepng  python  runScript.py  spl-lang-server-
ColdStorageArchiver_GCP.py  compsup  genWebCert.py  locktest  openssl  prigreypng  python3  safe_restart_cluster_master.py  spl2-orchestrato
Sbenchmark  copyright.txt  genWebCert.py  mongod  parse_zul_buckets.py  pripalpng  python3.7  scripts  splunk
blame  dbmanipulator.py  genWebCert.sh  mongod-3.6  pcra2-config  pripanotpng  python3.7a  scrubber.py  splunk-optimize-
bottle.py  easy_install-3.7  idle3  mongod-4.0  pcregextest  pripnglsch  pyvenv  searchtest  splunk-optimize-
btool  exporttool  idle3.7  mongodump  pid_check.sh  pripngtopam  pyvenv-3.7  setSplunkEnv  splunk-tlsd
bitprobe  fill_summary_index.py  importtool  mongorestore  pip3.7  priweavepng  rapid0tag  she_upgrade_template.py  splunkd
brp2  genAuditKeys.py  installit.py  mongorestore  pip3.7  pydoc3  recover-metadata  signtool  splunkmon
```

Iniciamos splunk ejecutando el comando “*./splunk start --accept-license*”:

```
(root@kali)~/opt/splunk/bin
# ./splunk start --accept-license

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:
```

Ponemos el nombre del usuario y la contraseña que deseemos a Splunk y nos lo apuntamos en un lugar seguro para recordarlo posteriormente.

```
done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
Writing new private key to 'privKeySecure.pem'

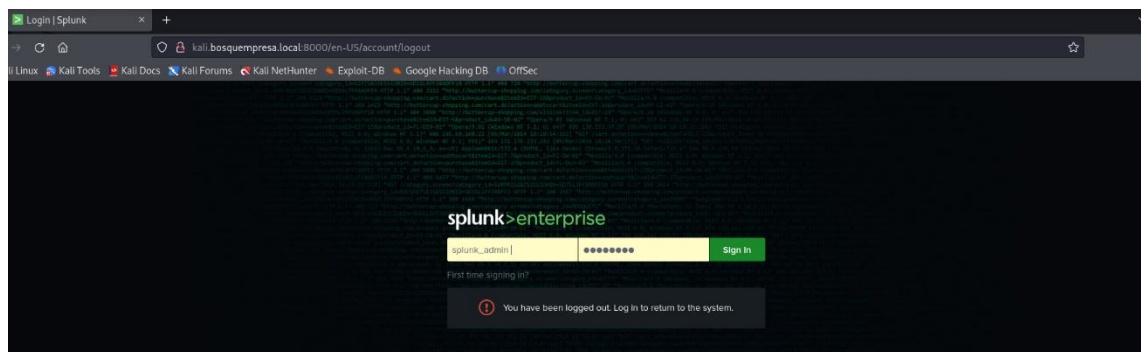
Signature ok
subject=/CN=kali.bosquempresa.local/O=SplunkUser
Getting CA Private Key
Writing RSA key
YTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for one
one

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

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.bosquempresa.local:8000
```

Al finalizar la ejecución del comando anterior, nos saldrá esta url, que debemos pegar en nuestro navegador web para acceder al dashboard.



Ahora vamos a nuestra máquina virtual Windows 10 y nos aseguramos de que ambas máquinas estén en la misma red:

```
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Admin\ipconfig

Configuración IP de Windows

Adaptador de Ethernet LAN:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::f38e:7cd3:d940:6a64%9
    Dirección IPv4. . . . . : 192.168.1.135
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.1.1

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::3ab3:57d0:210e:f459%3
    Dirección IPv4 de configuración automática: 169.254.114.31
    Máscara de subred. . . . . : 255.255.0.0
    Puerta de enlace predeterminada. . . . . :

C:\Users\Admin>
```

```
(root@kali)-[/opt/splunk/bin]
# ifconfig
br-729cb46222df: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
    inet6 fe80::42:51ff:fe55:b13c prefixlen 64 scopeid 0x20<link>
    ether 02:42:51:55:b1:3c txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 2276 (2.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:65ff:fe23:385 prefixlen 64 scopeid 0x20<link>
    ether 02:42:65:23:03:85 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 2276 (2.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
    inet 192.168.1.133 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::e76f:715e:3495:83af prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c4:a0:a1 txqueuelen 1000 (Ethernet)
    RX packets 891225 bytes 1268378315 (1.1 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33698 bytes 3113315 (2.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Vemos que la IP de nuestra máquina virtual Windows 10 es 192.168.1.135 y la IP de nuestra máquina virtual Kali Linux es 192.168.1.133, por lo tanto, están en la misma red.

Haremos *ping* de una máquina a la otra para asegurarnos de que exista la comunicación entre ambas. Primero hacemos de nuestra máquina Kali a Windows 10:

```
(root@kali)-[/opt/splunk/bin]
# ping 192.168.1.135
PING 192.168.1.135 (192.168.1.135) 56(84) bytes of data.
64 bytes from 192.168.1.135: icmp_seq=1 ttl=128 time=3.70 ms
64 bytes from 192.168.1.135: icmp_seq=2 ttl=128 time=1.28 ms
64 bytes from 192.168.1.135: icmp_seq=3 ttl=128 time=1.19 ms
64 bytes from 192.168.1.135: icmp_seq=4 ttl=128 time=5.67 ms
64 bytes from 192.168.1.135: icmp_seq=5 ttl=128 time=1.88 ms
64 bytes from 192.168.1.135: icmp_seq=6 ttl=128 time=1.65 ms
64 bytes from 192.168.1.135: icmp_seq=7 ttl=128 time=2.06 ms
64 bytes from 192.168.1.135: icmp_seq=8 ttl=128 time=1.61 ms

64 bytes from 192.168.1.135: icmp_seq=9 ttl=128 time=2.16 ms
64 bytes from 192.168.1.135: icmp_seq=10 ttl=128 time=2.74 ms
^Z
zsh: suspended ping 192.168.1.135
```

Y ahora hacemos ping de nuestra máquina virtual Windows 10 a Kali:

```
Símbolo del sistema

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::3ab3:57d0:210e:f459%3
    Dirección IPv4 de configuración automática: 169.254.114.31
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada . . . . . :

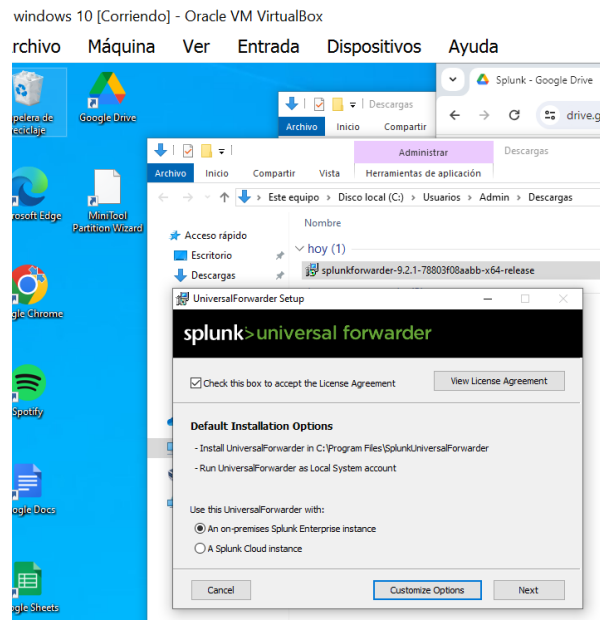
C:\Users\Admin>ping 192.168.1.133

Haciendo ping a 192.168.1.133 con 32 bytes de datos:
Respuesta desde 192.168.1.133: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.133: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.133: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.133: bytes=32 tiempo=2ms TTL=64

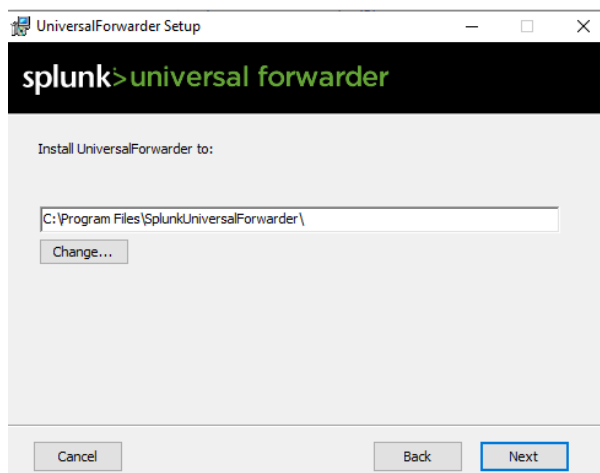
Estadísticas de ping para 192.168.1.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 1ms
```


Ping ejecutado correctamente en ambas máquinas, por lo tanto, podemos decir que la conectividad entre ambas es correcta.

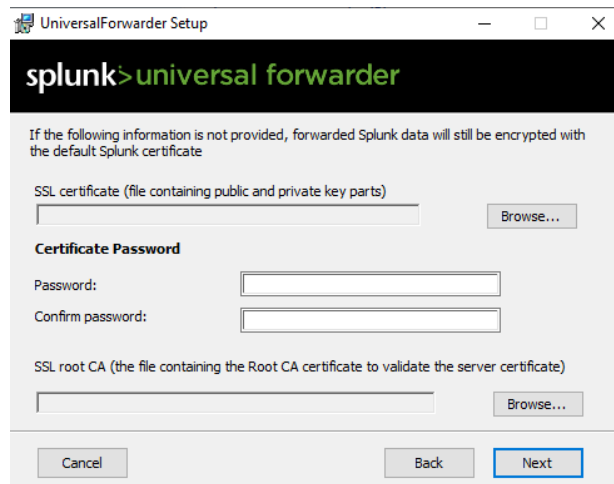
Ahora en nuestra máquina virtual Windows 10 nos descargamos la versión *Splunk Universal Forwarder* más reciente desde la página oficial y procedemos a su instalación:



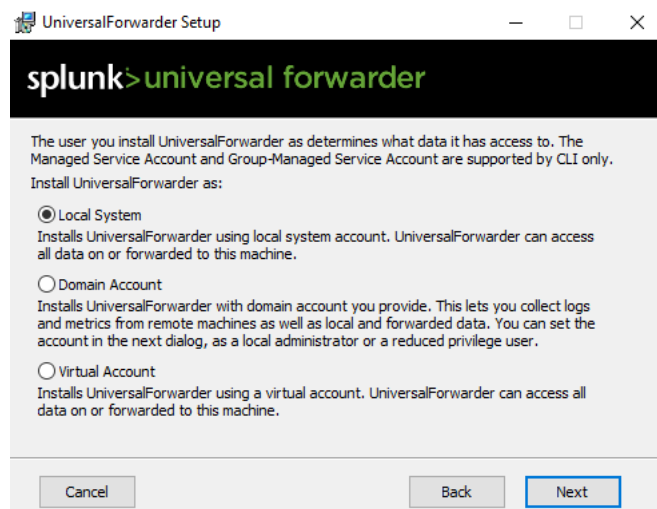
Seleccionamos la casilla de arriba y presionamos en *Customize Options*:



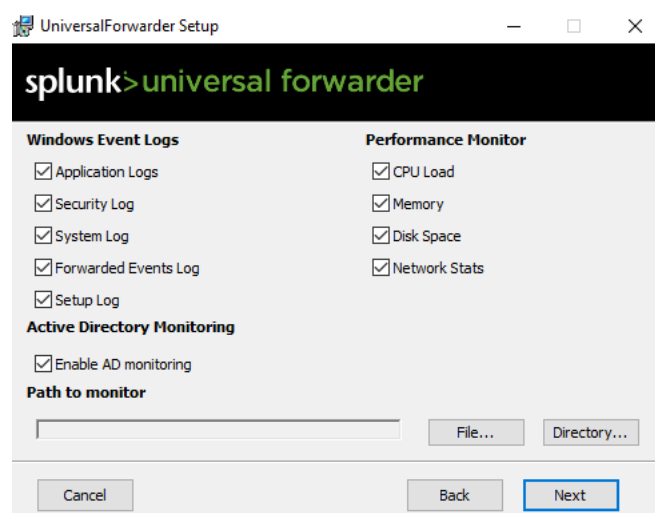
Seleccionamos el directorio para su instalación y presionamos *Next*:



En este paso no es necesario rellenar ninguna casilla, así que presionamos *Next*:



Seleccionamos la opción Local System y presionamos *Next*:



Seleccionamos todo y le damos a *Next* para crear las credenciales para la cuenta de administrador:

UniversalForwarder Setup

splunk>universal forwarder

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

Username:
splunk_user

☐ Generate random password

Password:
••••••••

Confirm password:
••••••••

Cancel Back 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
192.168.1.133 :

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

Cancel Back Next

Escribimos la IP de nuestro Kali, la cual es 192.168.1.133, sin especificar el puerto, ya que obtiene el 8089 por defecto.

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.

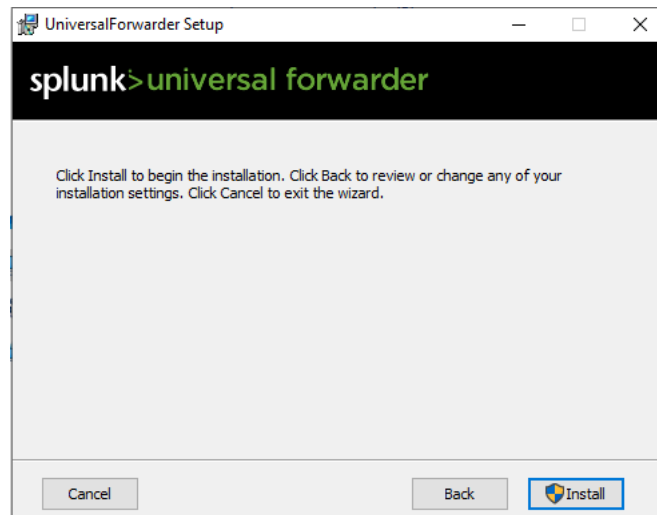
Receiving Indexer

Hostname or IP
192.168.1.133 : 9997

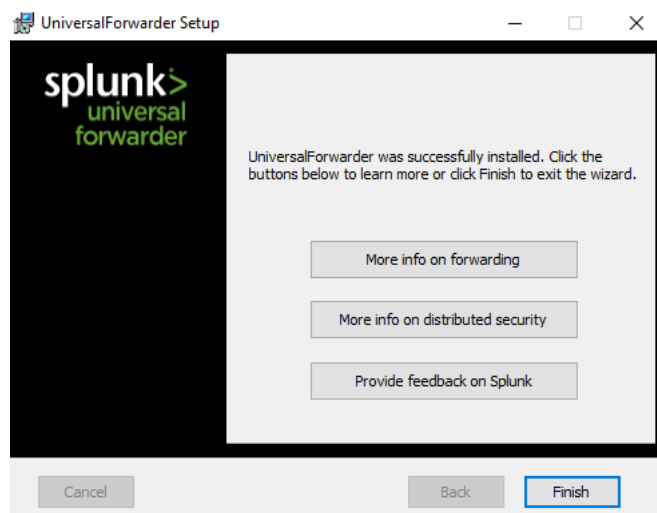
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

Cancel Back Next

Aquí volvemos a escribir la IP de nuestro Kali y especificamos el puerto para evitar posibles problemas.

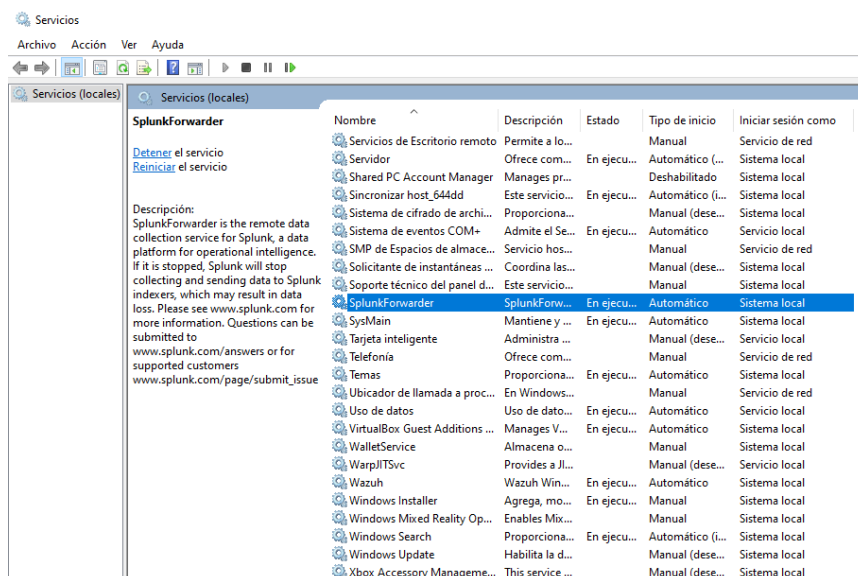


Le damos a *Install*.



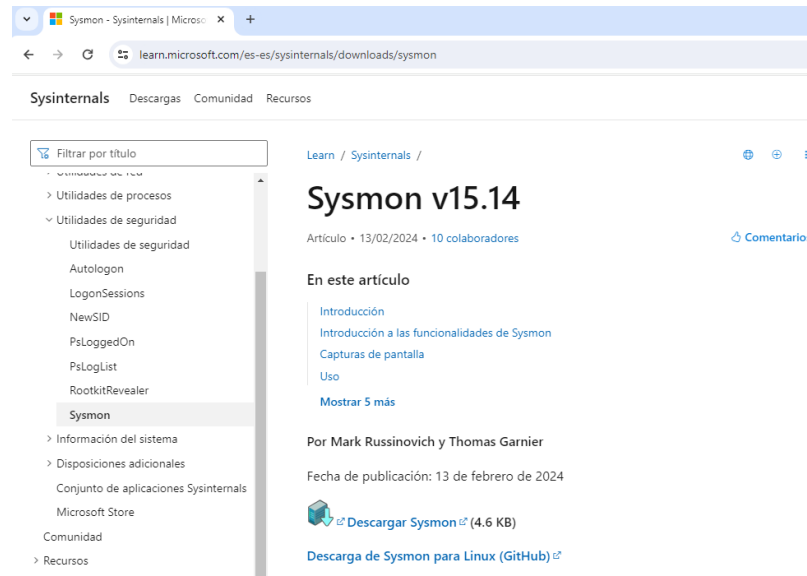
Instalado correctamente, presionamos *Finish*.

Ahora, nos dirigimos a Servicios para comprobar que se haya instalado correctamente:

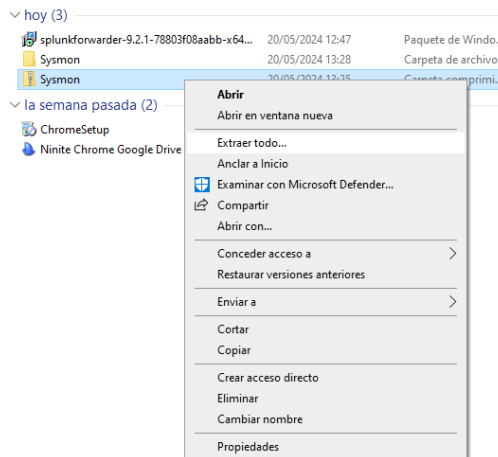


2. Instalación y Configuración de Sysmon en Máquina Windows

Nos descargamos Sysmon desde la página oficial:



Descomprimos el archivo zip descargado y extraemos los ficheros:



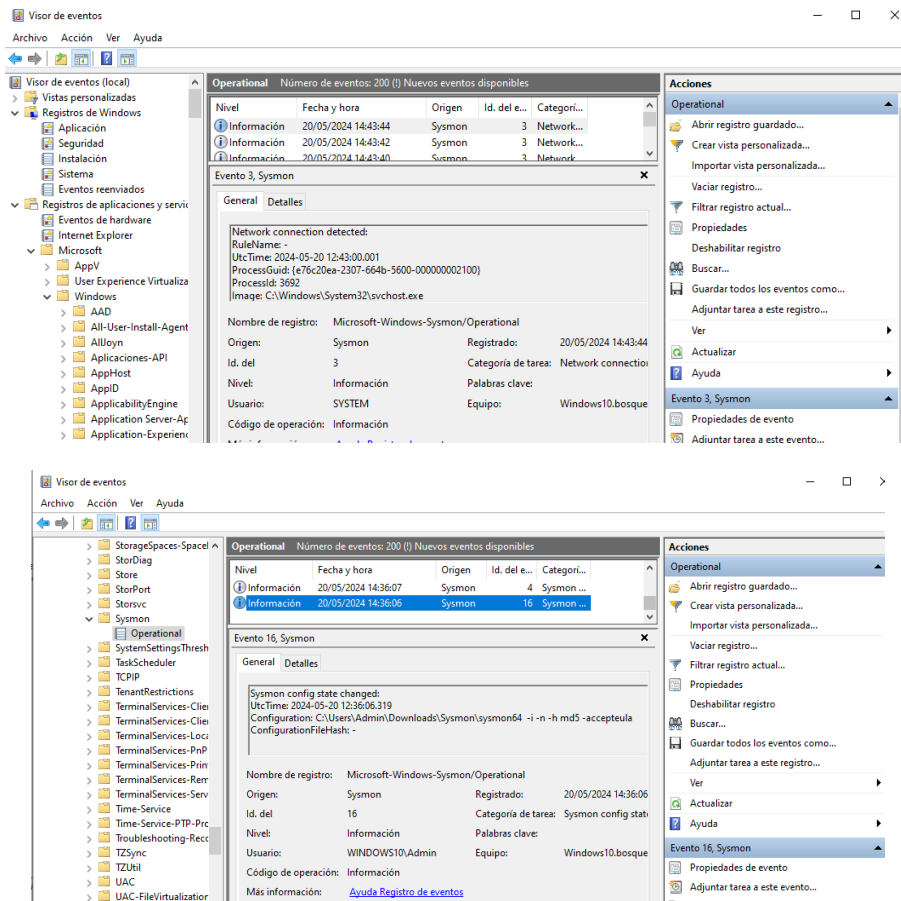
El comando que debemos utilizar para su instalación es “sysmon64 -i -n -h md5 -accepteula”:

```
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.
```

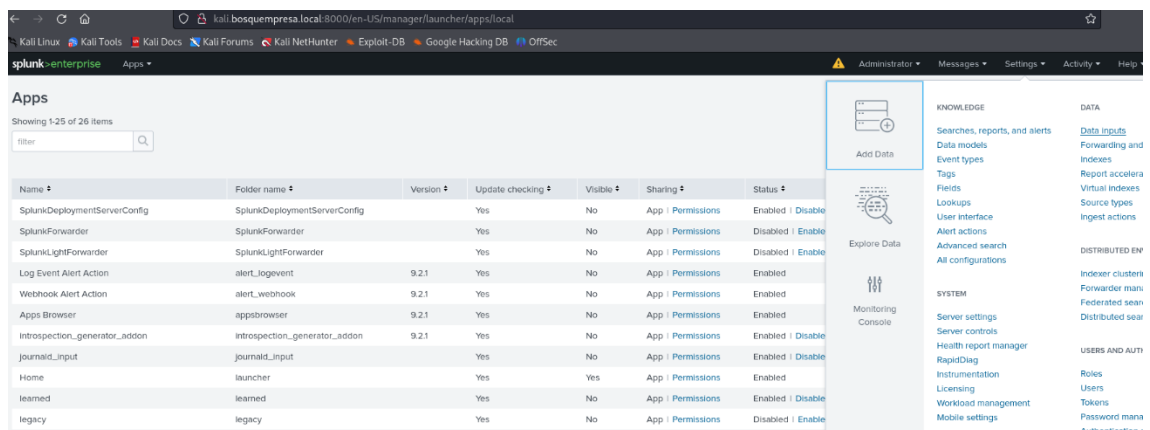
Para verificar que Sysmon está funcionando y generando eventos en el visor de eventos de Windows, nos iremos a la carpeta Registro de aplicaciones y servicios → Microsoft → Windows. Buscaremos la carpeta Sysmon y seleccionaremos el fichero *Operational*:



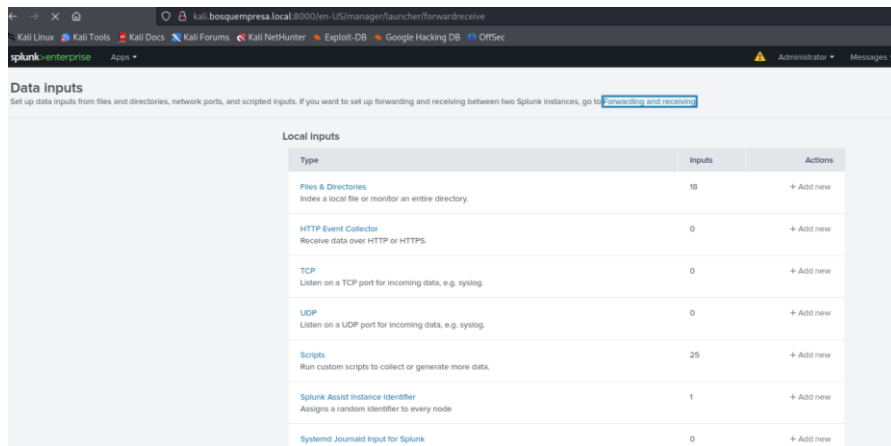
Aquí dentro podemos ver los eventos que se están generando. Por ejemplo, el que está seleccionado es el primer evento que se ha generado, llamado evento de configuración y corresponde a la ejecución del comando para su instalación.

3. Configuración de Splunk para Recibir Eventos de Sysmon

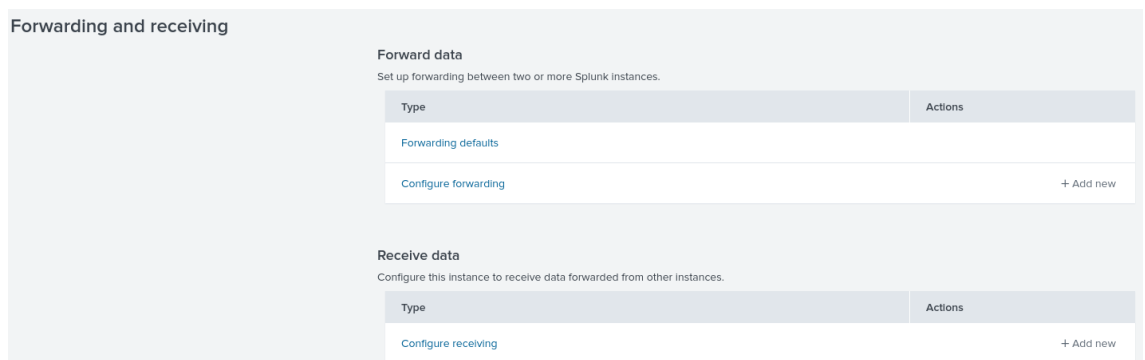
Nos dirigimos a *Settings* → *Data Inputs*:



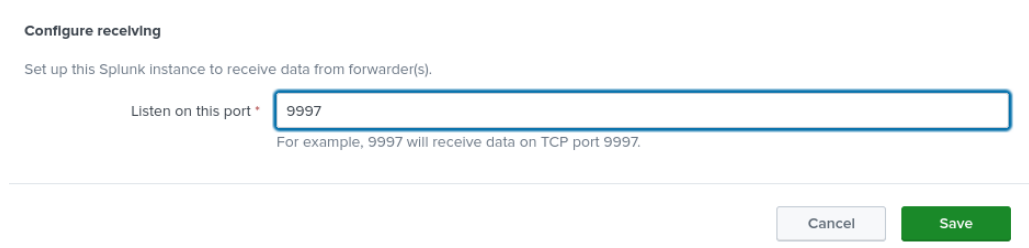
Clicamos en *Forwarding and receiving*:



Clicamos en *+Add new* de *Configure receiving*:



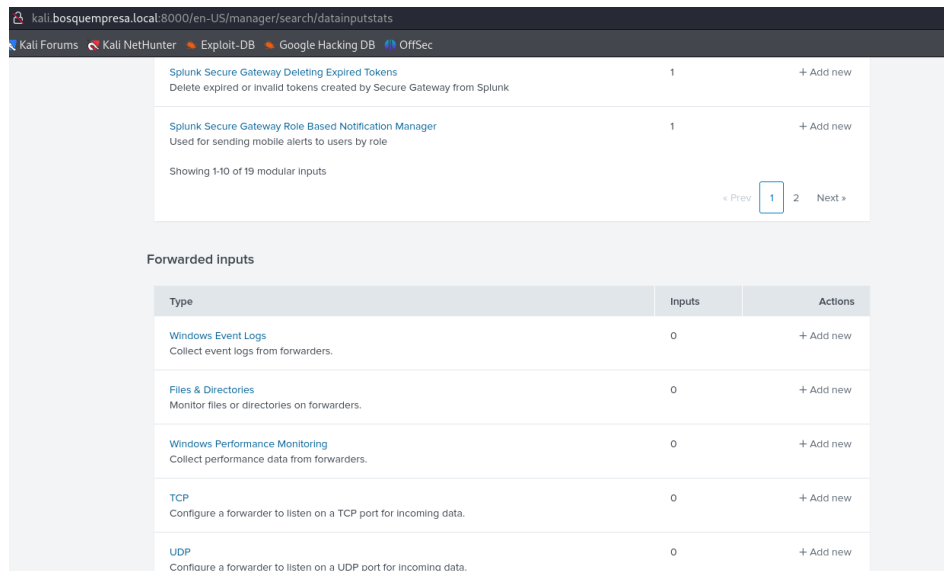
Añadimos el puerto 9997 y guardamos:



Ahora en la consola de Kali ejecutamos el comando “lsof -i:9997” para comprobar que exista la escucha con dicho puerto:

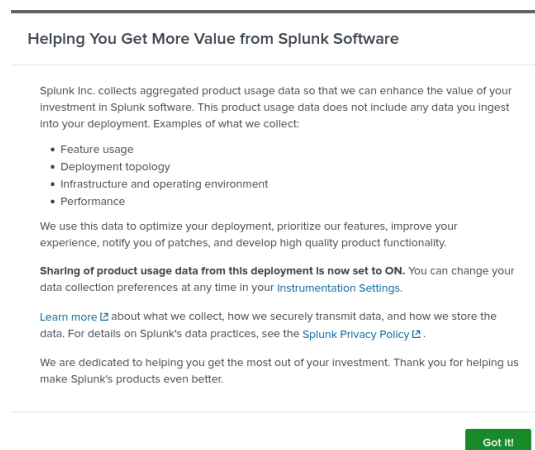
```
(root@kali)-[/opt/splunk/bin]
# lsof -i:9997
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF  NODE NAME
splunkd 3045 root 122u IPv4 395487      0t0  TCP 192.168.1.133:9997→192.168.1.135:52209 (ESTABLISHED)
splunkd 3045 root 189u IPv4 394008      0t0  TCP *:9997 (LISTEN)
```

Nos dirigimos nuevamente a *Settings* → *Data Inputs* → *Forwarded Inputs* y clicamos en *+Add new de Windows Events Logs*:



Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	+ Add new
Files & Directories Monitor files or directories on forwarders.	0	+ Add new
Windows Performance Monitoring Collect performance data from forwarders.	0	+ Add new
TCP Configure a forwarder to listen on a TCP port for incoming data.	0	+ Add new
UDP Configure a forwarder to listen on a UDP port for incoming data.	0	+ Add new

Clicamos en *Got it*:



Helping You Get More Value from Splunk Software

Splunk Inc. collects aggregated product usage data so that we can enhance the value of your investment in Splunk software. This product usage data does not include any data you ingest into your deployment. Examples of what we collect:

- Feature usage
- Deployment topology
- Infrastructure and operating environment
- Performance

We use this data to optimize your deployment, prioritize our features, improve your experience, notify you of patches, and develop high quality product functionality.

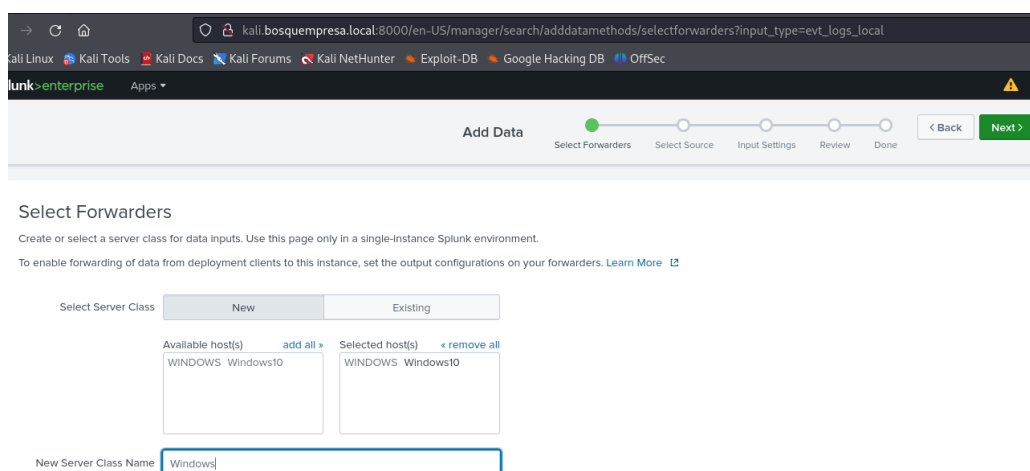
Sharing of product usage data from this deployment is now set to **ON**. You can change your data collection preferences at any time in your [Instrumentation Settings](#).

[Learn more](#) about what we collect, how we securely transmit data, and how we store the data. For details on Splunk's data practices, see the [Splunk Privacy Policy](#).

We are dedicated to helping you get the most out of your investment. Thank you for helping us make Splunk's products even better.

Got it!

Añadimos WINDOWS W10 clicando en *add all* y le ponemos el nombre de Windows al *New Server Class Name*. Pasamos al siguiente paso clicando en *Next*:



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 More](#)

Select Server Class

New	Existing
Available host(s) add all WINDOWS Windows10	Selected host(s) remove all WINDOWS Windows10

New Server Class Name

Añadimos todo con *add all* y seguimos al siguiente paso con *Next*:

The screenshot shows the 'Add Data' wizard in the Splunk interface, specifically the 'Select Source' step. The progress bar at the top indicates the current step. The main content area is titled '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](#)

On the left, there are several input types listed: 'file, or monitor an entire directory.', 'orm to listen on a network port.', 'vice, or database with a script.', 'Identifier', 't for Splunk', and 'nk platform'. The 'Identifier' and 't for Splunk' options are highlighted.

In the center, there is a 'Select Event Logs' section. It contains a list of 'Available item(s)' with the following items: 'Application', 'ForwardedEvents', 'Security', 'Setup', and 'Custom...'. An 'add all >' button is next to the list. Below the list, it says 'Select the Windows Event Logs you want to index from the list.'

On the right, there is a 'Selected item' section with a list of items: 'Application', 'ForwardedE', 'Security', 'Setup', and 'Custom...'. The 'Application' item is selected.

At the bottom, there is an 'FAQ' section with two questions: 'What event logs does this Splunk platform instance have access to?' and 'What is the best method for monitoring event logs of remote Windows machines?'.

Seguimos al siguiente paso clicando en *Review*, ya que no es necesario crear un nuevo índice:

The screenshot shows the 'Add Data' wizard in the Splunk interface, specifically the 'Input Settings' step. The progress bar at the top indicates the current step. The main content area is titled 'Input Settings' and contains the text 'Optionally set additional input parameters for this data input as follows:'. Below this, there is an 'Index' section. It contains the text '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](#)

On the right, there is an 'Index' dropdown menu with 'Default' selected. Next to it is a 'Create a new index' button.

At the bottom, there is an 'FAQ' section with two questions: 'How do indexes work?' and 'How do I know when to create or use multiple indexes?'.

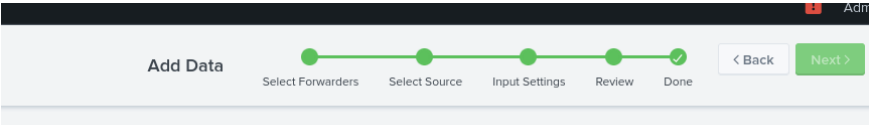
Por último, clicamos en *Submit*:

The screenshot shows the 'Add Data' wizard in the Splunk interface, specifically the 'Review' step. The progress bar at the top indicates the current step. The main content area is titled 'Review' and contains the following fields:

- 'Server Class Name' with the value 'Windows'.
- 'List of Forwarders' with the value 'WINDOWS | Windows10'.
- 'Collection Name' with the value 'localhost'.
- 'Input Type' with the value 'Windows Event Logs'.
- 'Event Logs' with a list of items: 'Application', 'ForwardedEvents', 'Security', 'Setup', and 'System'.
- 'Index' with the value 'default'.

At the bottom, there is a 'Submit' button.

Ahora, le damos a *Start Searching* para empezar a ver todos los eventos en el *Dashboard*:



✓ Local event logs input has been created successfully.
Configure your inputs by going to Settings > Data Inputs

Start Searching

 Search your data now or see [examples and tutorials](#).

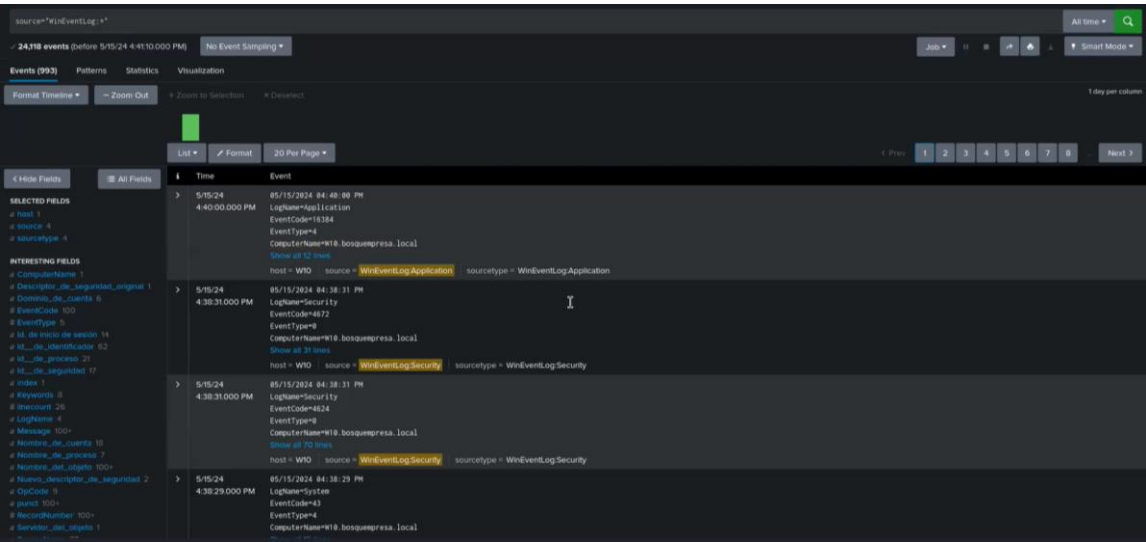
Add More Data

 Add more data inputs now or see [examples and tutorials](#).

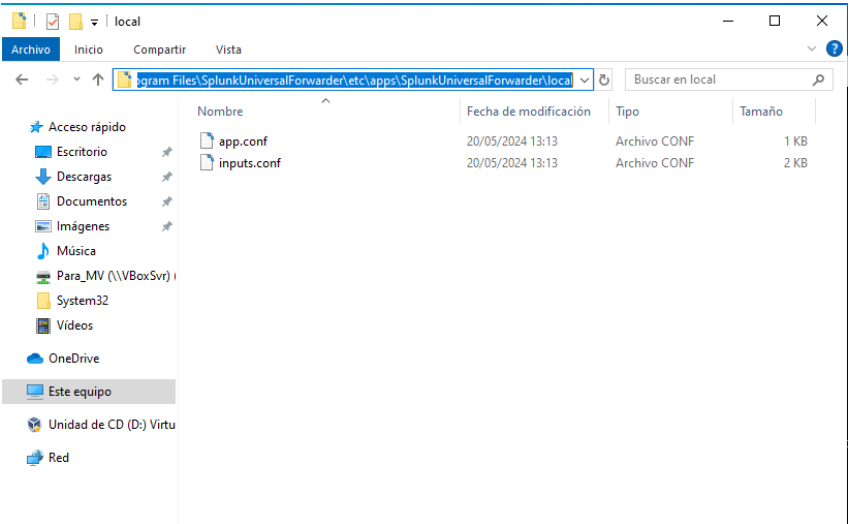
Download Apps

 Apps help you do more with your data. [Learn more](#).

Build Dashboards

 Visualize your searches. [Learn more](#).

En Windows 10 de la máquina virtual vamos al directorio C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local y veremos dos archivos:



Abrimos el archivo *inputs.conf* y añadimos el siguiente código:

```
*inputs: Bloc de notas
Archivo Edición Formato Ver Ayuda
start_from = oldest

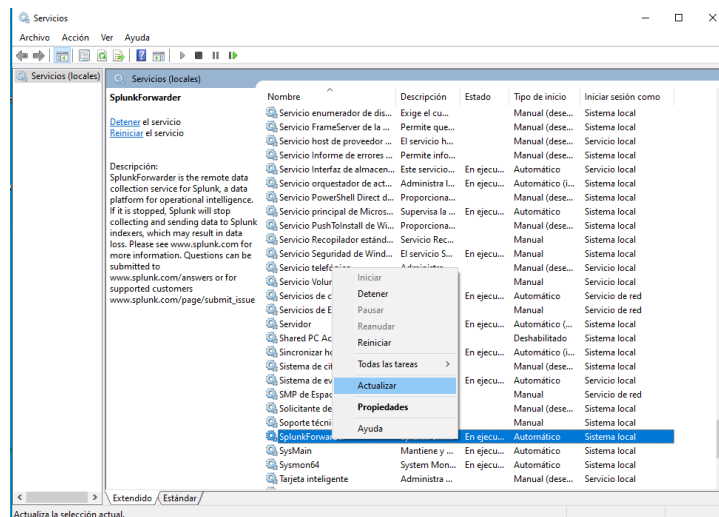
[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

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

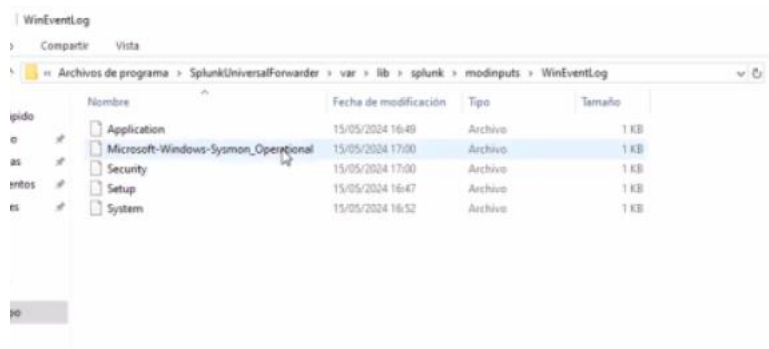
[WinEventLog://Setup]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest

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

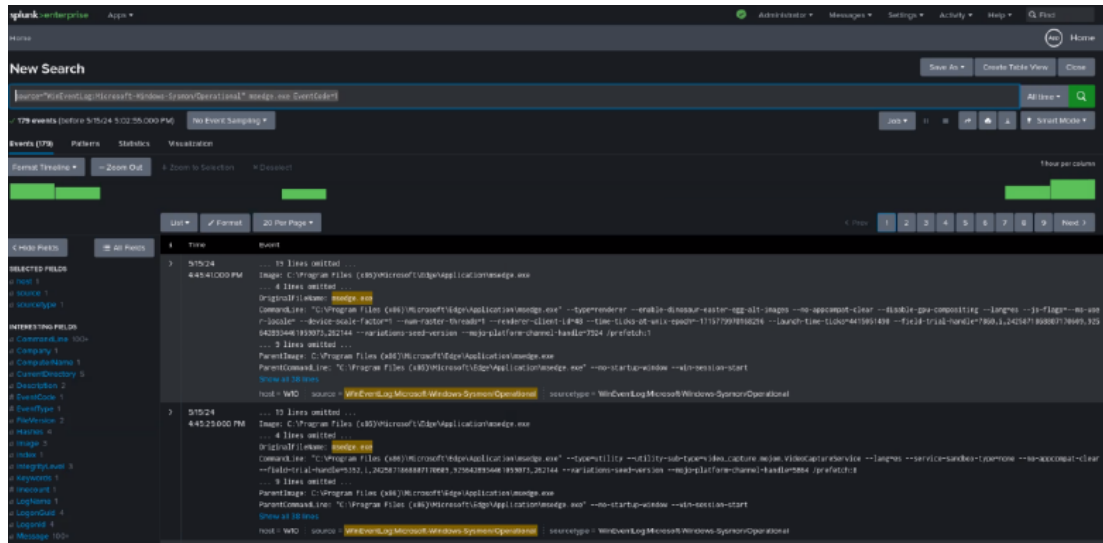
Ahora, en Windows 10 de la máquina virtual, vamos a Servicios y buscamos *SysmonForwarder*, clic derecho, actualizar:



Comprobamos que haya creado correctamente el servicio del paso anterior, para ello iremos al directorio: C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinputs\WinEventLog

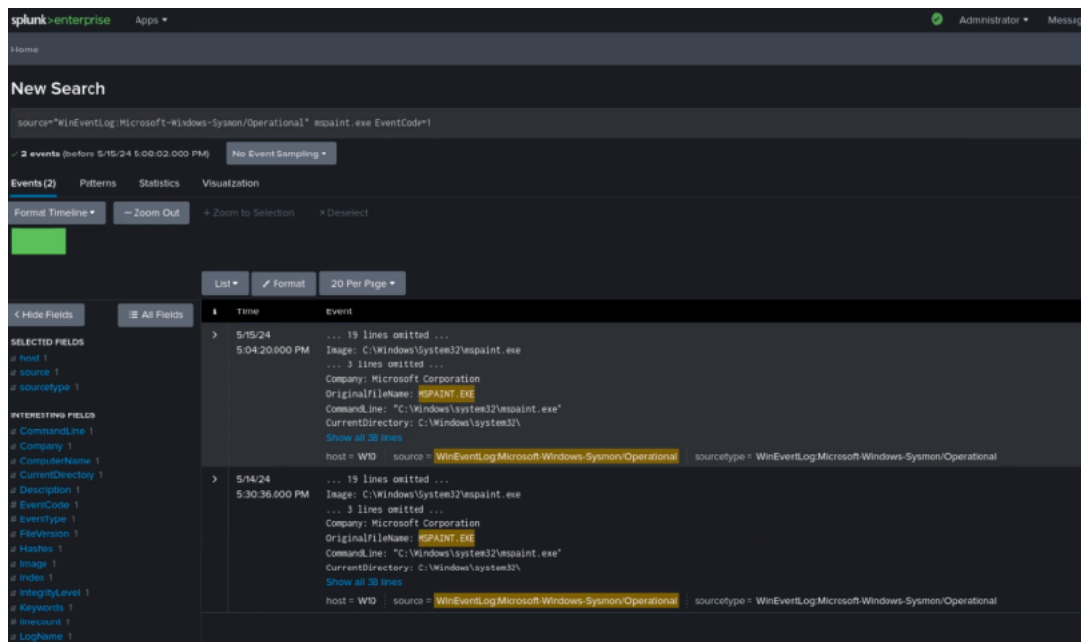


Nos aseguramos de que Splunk está recibiendo los eventos de Sysmon correctamente revisando los índices de datos en el dashboard de Splunk mediante el comando: `source="WinEventLog:Microsoft-Windows-Sysmon_Operational" msedge.exe EventCode=1`



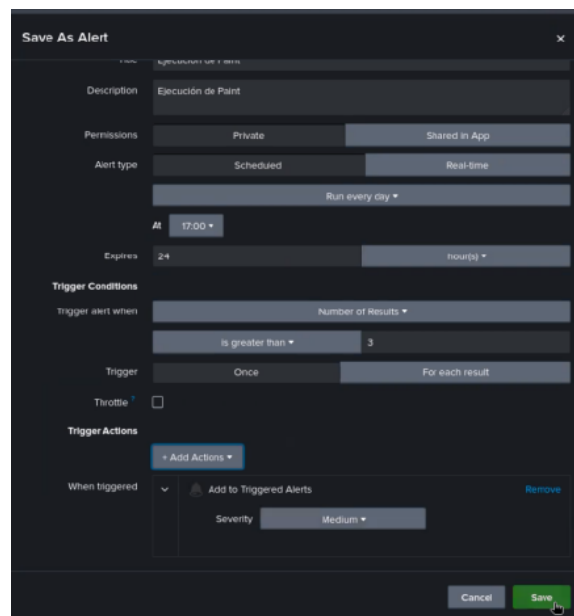
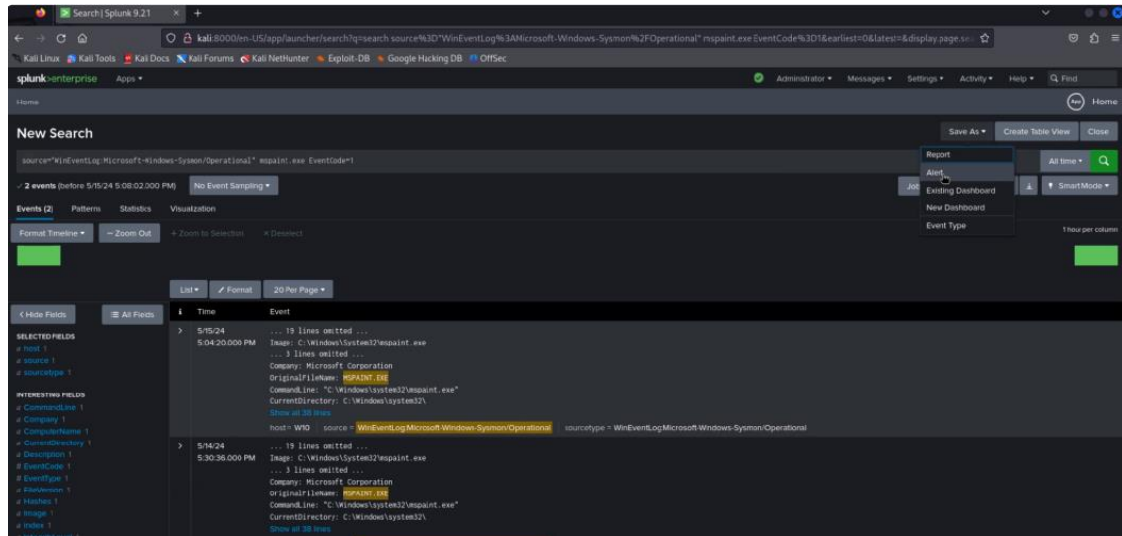
4. Generación de Eventos de Seguridad

En Windows 10 de VirtualBox ejecutamos Paint para así generar logs, los cuales luego buscaremos en Splunk mediante el comando: `source="WinEventLog:Microsoft-Windows-Sysmon/Operational" mspaint.exe EventCode=1`



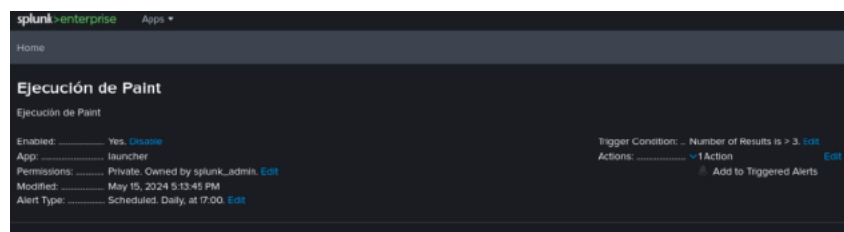
5. Análisis de Eventos en Splunk

Podemos configurar alertas para identificar la apertura de aplicaciones concretas. Para ello iremos a la pestaña *Save As* y clicamos en *Alert*:



Añadimos una acción indispensable y le damos a guardar.

Seguidamente nos saldrán los detalles de la alerta creada y cuando se produzca la alerta recibiremos un mensaje.



Buen trabajo !!!!

10/10