Actividad de clase: Identificar procesos en ejecución (versión para el instructor)

**Nota para el instructor**: Los elementos con color de fuente rojo o resaltados en gris indican texto que aparece solo en la copia del instructor.

# Objetivos

En esta práctica de laboratorio utilizarán el Visor de terminales TCP/UDP, una herramienta de la suite Sysinternals, para identificar cualquier proceso en ejecución en su computadora.

Parte 1: Descargue Windows Sysinternals Suite.

Parte 2: Inicie el visualizador de terminal TCP/UDP

Parte 3: Explore los procesos de ejecución

Parte 4: Explore un proceso iniciado por el usuario.

# Antecedentes / Escenario

En esta práctica de laboratorio estudiarán procesos. Los procesos son programas o aplicaciones en ejecución. Estudiarán los procesos con el Explorador de procesos en la suite Sysinternals para Windows. También iniciarán y observarán un proceso nuevo.

# Recursos necesarios

* 1 Una PC Windows con acceso a internet

# Instrucciones

## Descarguen la suite Sysinternals para Windows.

* + 1. Diríjanse al siguiente enlace para descargar la suite Sysinternals para Windows:

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

* + 1. Una vez finalizada la descarga, hagan clic derecho sobre el archivo zip y elijan **Extract All…** (Extraer todo) para extraer los archivos a la carpeta. Elijan el nombre y el destino predeterminados en la carpeta (Downloads) Descargas y hagan clic en **Extract** (Extraer).
    2. Salgan del navegador web

## Inicien el Visor de terminales TCP/UDP.

* + 1. Diríjanse a la carpeta SysinternalsSuite con todos los archivos extraídos.
    2. Abran **Tcpview.exe**. Acepten el Acuerdo de licencia de Process Wxplorer cuando el sistema se lo solicite. Hagan clic en **Yes** (Sí) para permitir que esta aplicación realice cambios en sus dispositivos.
    3. Salgan del Explorador de archivos y cierren todas las aplicaciones en ejecución.

## Estudien los procesos en ejecución.

* + 1. TCPView incluye en una lista los procesos que se encuentran en este momento en su PC Windows. En este instante, solo se están ejecutando procesos de Windows.
    2. Hagan doble clic en **lsass.exe**.

### Pregunta:

¿Qué es lsass.exe? ¿En qué carpeta está ubicado?

Escriba sus respuestas aquí.

Proceso de autoridad de seguridad local es el nombre para lsass.exe. Se encuentra en la carpeta C:\Windows\System32\.

* + 1. Cierren la venta de propiedades correspondiente a lsass.exe cuando hayan terminado.
    2. Miren las propiedades correspondientes a los otros procesos en ejecución.

**Nota**: No se puede consultar la información de las propiedades correspondiente a todos los procesos.

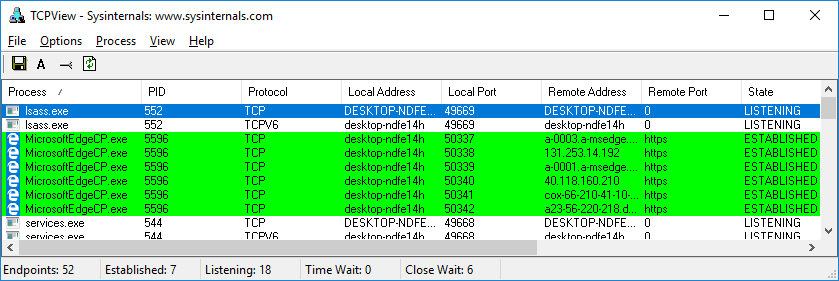
## Estudien un proceso iniciado por el usuario.

* + 1. Abra un navegador web, como Microsoft Edge.

¿Qué observaron en la ventana de TCPView?

Escriba sus respuestas aquí.

Los procesos para el navegador web se agregan a la ventana de TCPView.



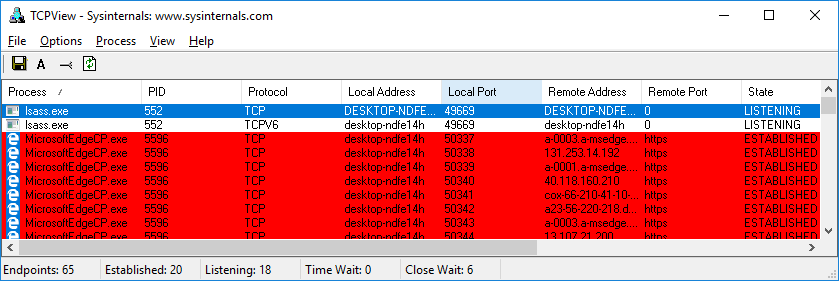
* + 1. Cierre el navegador web.

### Pregunta:

¿Qué observaron en la ventana de TCPView?

Escriba sus respuestas aquí.

Los procesos para el navegador web se eliminarán de la ventana de TCPView.



* + 1. Vuelvan a abrir el navegador web. Estudien algunos de los procesos de la lista de TCPView. Registre sus conclusiones.

Escriba sus respuestas aquí.

Las respuestas pueden variar. El proceso lsass.exe comprueba la validez de los inicios de sesión de usuario en la PC. El ejecutable services.exe se utiliza para iniciar y detener servicios y cambiar la configuración predeterminada del inicio de servicios. El proceso svnhost.exe (host de servicio) maneja el proceso de compartir recursos del sistema. La mayoría de estos recursos mencionados se encuentra en la carpeta C:\Windows\System32\. Si estos ejecutables se encuentran en otras partes del sistema, tal vez malware, como virus, spyware, troyanos o gusanos.

Fin del documento