

Actividad de clase: Identificar procesos en ejecución

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

Parte 1: Descarguen la suite Sysinternals para Windows.

- Diríjense al siguiente enlace para descargar la suite Sysinternals para Windows:
<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- 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).
- Salgan del navegador web

Parte 2: Inicien el Visor de terminales TCP/UDP.

- Diríjense a la carpeta SysinternalsSuite con todos los archivos extraídos.
- 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.
- Salgan del Explorador de archivos y cierren todas las aplicaciones en ejecución.

Parte 3: Estudien los procesos en ejecución.

- 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.
- Hagan doble clic en **lsass.exe**.
¿Qué es lsass.exe? ¿En qué carpeta está ubicado?

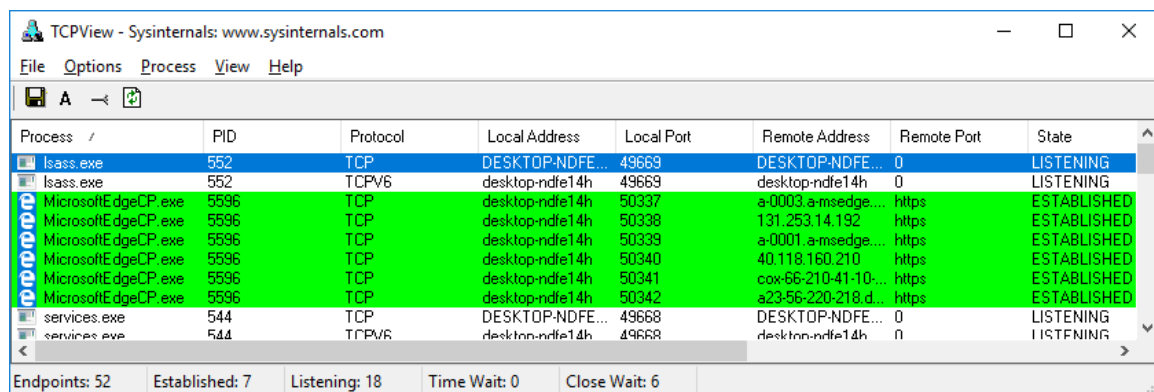
- c. Cierren la venta de propiedades correspondiente a lsass.exe cuando hayan terminado.
- d. Miren las propiedades correspondientes a los otros procesos en ejecución.

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

Parte 4: Estudien un proceso iniciado por el usuario.

- a. Abra un navegador web, como Microsoft Edge.

¿Qué observaron en la ventana de TCPView?



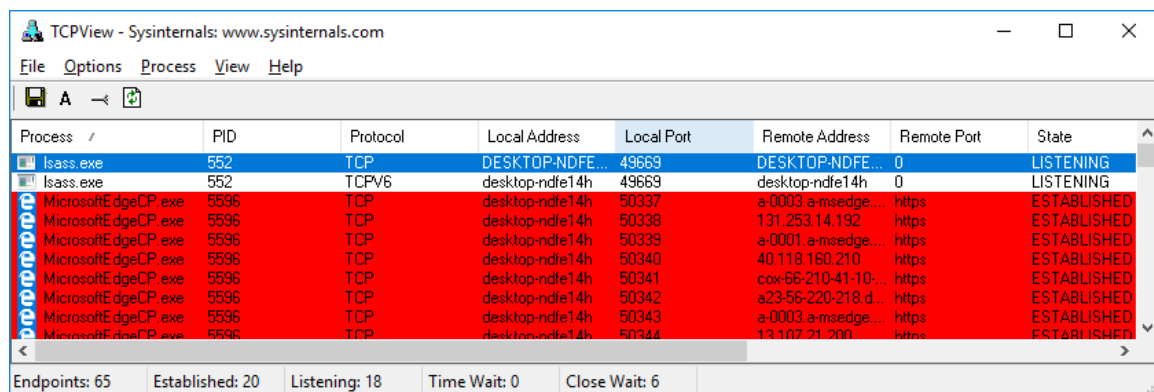
The screenshot shows the TCPView application window. The process list on the left includes lsass.exe and several instances of Microsoft EdgeCP.exe. The main table displays network connections. lsass.exe is listening on port 49669. Microsoft Edge is established on various ports (50337-50342) connecting to different remote addresses. The status bar at the bottom shows 52 endpoints, 7 established, and 18 listening.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
lsass.exe	552	TCPV6	desktop-ndfe14h	49669	desktop-ndfe14h	0	LISTENING
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50337	a-0003.a-msedge...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50338	131.253.14.192	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50339	a-0001.a-msedge...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50340	40.118.160.210	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50341	cox-66-210-41-10...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50342	a23-56-220-218.d...	https	ESTABLISHED
services.exe	544	TCP	DESKTOP-NDFE...	49668	DESKTOP-NDFE...	0	LISTENING
services.exe	544	TCPV6	desktop-ndfe14h	49668	desktop-ndfe14h	0	LISTENING

Endpoints: 52 Established: 7 Listening: 18 Time Wait: 0 Close Wait: 6

- b. Cierre el navegador web.

¿Qué observaron en la ventana de TCPView?



The screenshot shows the TCPView application window after closing the browser. The process list on the left still includes Microsoft EdgeCP.exe. The main table shows that the previously established connections for Microsoft Edge are now in a 'CLOSE_WAIT' state. The status bar at the bottom shows 65 endpoints, 20 established, and 18 listening.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
lsass.exe	552	TCPV6	desktop-ndfe14h	49669	desktop-ndfe14h	0	LISTENING
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50337	a-0003.a-msedge...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50338	131.253.14.192	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50339	a-0001.a-msedge...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50340	40.118.160.210	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50341	cox-66-210-41-10...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50342	a23-56-220-218.d...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50343	a-0003.a-msedge...	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-ndfe14h	50344	13.107.21.200	https	ESTABLISHED

Endpoints: 65 Established: 20 Listening: 18 Time Wait: 0 Close Wait: 6

Actividad de clase: Identificar procesos en ejecución

- c. Vuelvan a abrir el navegador web. Estudien algunos de los procesos de la lista de TCPView. Registre sus conclusiones.