Tema3.3.0.3.EnriqueGomezTagle

lunes, 12 de febrero de 2024 23:20

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

Parte 3: Estudien los procesos en ejecución.

a. 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.

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

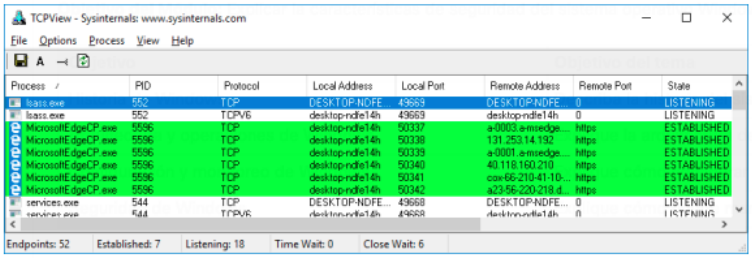
Servicio de subsistema de seguridad local, autenticacion de usuarios y politicas de seguridad.

C:\Windows\System32\lsass.exe

Parte 4: Estudien un proceso iniciado por el usuario.

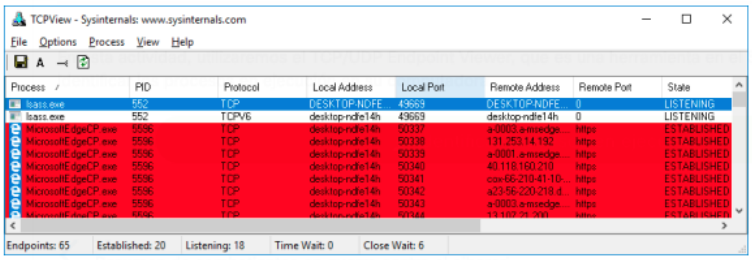
a. Abra un navegador web, como Microsoft Edge.
¿Qué observaron en la ventana de TCPView?

se agrega el proceso para Edge



b. Cierre el navegador web.
¿Qué observaron en la ventana de TCPView?

Desparece el proceso



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

TCP permite ver procesos en ejecución
Al iniciar proceso, se agrega, y al cerrar se elimina.