

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 (o c:\
utilización de usuarios y políticas 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 agregó el proceso para Edge

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	512	TCP	DESKTOPND14h	43693	DESKTOPND14h	0	LISTENING
lsass.exe	552	TCPV6	desktop-nd14h	43693	desktop-nd14h	0	LISTENING
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50337	a-0003 a-mesedge	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50338	131.253.14.192	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50339	a-0001 a-mesedge	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50340	40.118.160.210	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50341	cos66-210-41-10	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50342	a2356-220-218 d	https	ESTABLISHED
services.exe	544	TCP	DESKTOPNDFE...	43668	DESKTOPNDFE...	0	LISTENING
services.exe	544	TCPV6	desktop-nd14h	43668	desktop-nd14h	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?

Después el proceso

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	512	TCP	DESKTOPND14h	43693	DESKTOPND14h	0	LISTENING
lsass.exe	552	TCPV6	desktop-nd14h	43693	desktop-nd14h	0	LISTENING
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50337	a-0003 a-mesedge	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50338	131.253.14.192	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50339	a-0001 a-mesedge	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50340	40.118.160.210	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50341	cos66-210-41-10	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50342	a2356-220-218 d	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	50343	a-0003 a-mesedge	https	ESTABLISHED
MicrosoftEdgeCP.exe	5596	TCP	desktop-nd14h	49344	131.253.14.192	https	ESTABLISHED

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

- 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.

