

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCIA DIGITAL PRÁCTICA. IDENTIFICAR PROCESOS EN EJECUCIÓN

Departament d'informàtica.

Autor: Francisco Aldarias Raya

Julio-2023

Preparació
Proves
d'Accés

ÍNDEX

1 Introducción	2
2 Requisitos	2
3 Pasos	2
3.1 Instalar software	2
3.2 Iniciar app tcpviewer	2
3.3 Estudiar procesos que hay en ejecución	3
3.4 Estudiar procesos cuando se abre una app	3
3.5 Buscar herramientas similares en otros sistemas operativos.	3

1 Introducción

En la siguiente práctica se utilizará una app que permite ver información sobre los procesos en ejecución.

La práctica utilizará el software tcpviewer de Microsoft, pero existen herramientas similares en otros sistemas operativos como linux o mac.

En esta práctica se estudiarán procesos. Los procesos son programas en ejecución que están cargados en memoria RAM.

Veremos un fichero EULA, y practicaremos descomprimir archivos.

2 Requisitos

Se va a necesitar:

- Conexión a internet
- Windows
- App winzip

3 Pasos

3.1 Instalar software

1. Descargar en la carpeta descargas el fichero.zip del siguiente enlace la la suite Sysinternals para Windows:
<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
2. Una vez descargar el archivo, abrir el explorador de archivos extraer todos los documentos en una carpeta SysinternalsSuite.

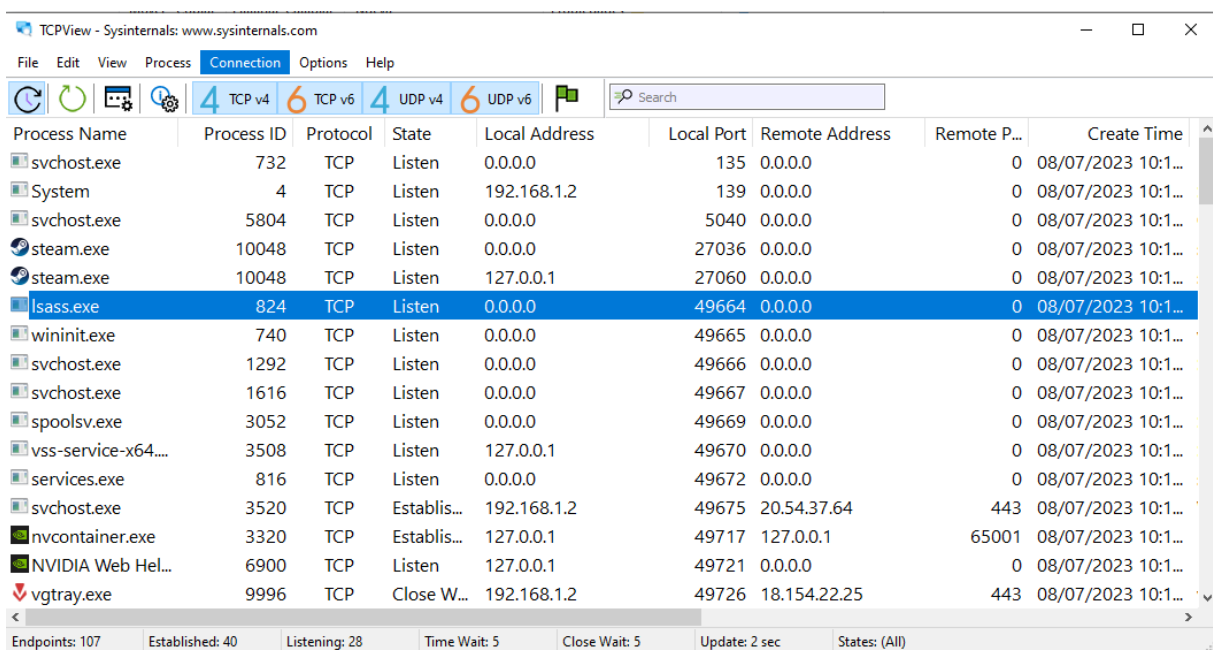
3.2 Iniciar app tcpviewer

1. Entrar en la carpeta SysinternalsSuite con todos los archivos. Comprueba el fichero EULA. Para que sirve este archivo? Qué te llama la atención?

2. Buscar la app tcpviewer.exe y ejecutarla pulsando dos veces. Diga Yes para permitir que la aplicación realice los cambios en tu dispositivo.
3. Salir del explorador y cerrar las aplicaciones abiertas excepto al app tcpview.

3.3 Estudiar procesos que hay en ejecución

1. TCPView incluye en una lista los procesos que se encuentran ahora en Windows. Ahora, solo se están ejecutando procesos del sistema operativo Windows.
2. Buscar el proceso en la app tcpview llamado lsass.exe y hacer doble click. Qué es ese proceso? En que carpeta se encuentra el fichero que lanzó el proceso?



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote P...	Create Time
svchost.exe	732	TCP	Listen	0.0.0.0	135	0.0.0.0	0	08/07/2023 10:1...
System	4	TCP	Listen	192.168.1.2	139	0.0.0.0	0	08/07/2023 10:1...
svchost.exe	5804	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	08/07/2023 10:1...
steam.exe	10048	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	08/07/2023 10:1...
steam.exe	10048	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	08/07/2023 10:1...
lsass.exe	824	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	08/07/2023 10:1...
wininit.exe	740	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	08/07/2023 10:1...
svchost.exe	1292	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	08/07/2023 10:1...
svchost.exe	1616	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	08/07/2023 10:1...
spoolsv.exe	3052	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	08/07/2023 10:1...
vss-service-x64....	3508	TCP	Listen	127.0.0.1	49670	0.0.0.0	0	08/07/2023 10:1...
services.exe	816	TCP	Listen	0.0.0.0	49672	0.0.0.0	0	08/07/2023 10:1...
svchost.exe	3520	TCP	Establis...	192.168.1.2	49675	20.54.37.64	443	08/07/2023 10:1...
nvcontainer.exe	3320	TCP	Establis...	127.0.0.1	49717	127.0.0.1	65001	08/07/2023 10:1...
NVIDIA Web Hel...	6900	TCP	Listen	127.0.0.1	49721	0.0.0.0	0	08/07/2023 10:1...
vgtray.exe	9996	TCP	Close W...	192.168.1.2	49726	18.154.22.25	443	08/07/2023 10:1...

Endpoints: 107 Established: 40 Listening: 28 Time Wait: 5 Close Wait: 5 Update: 2 sec States: (All)

3. Cerra la ventana de propiedades del proceso lsass.exe cuando termines.
4. Mirar propiedades de otros procesos. (Nota: Hay procesos que no permite ver sus propiedades)

3.4 Estudiar procesos cuando se abre una app

1. Abrir el navegador Microsoft Edge. ¿Qué observas en la ventana de tcpview?
2. Cerrar el navegador web. ¿Qué observas en la ventana de TCPView?

3.5 Buscar herramientas similares en otros sistemas operativos.

Si has encontrado alguna indica cuales