

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.

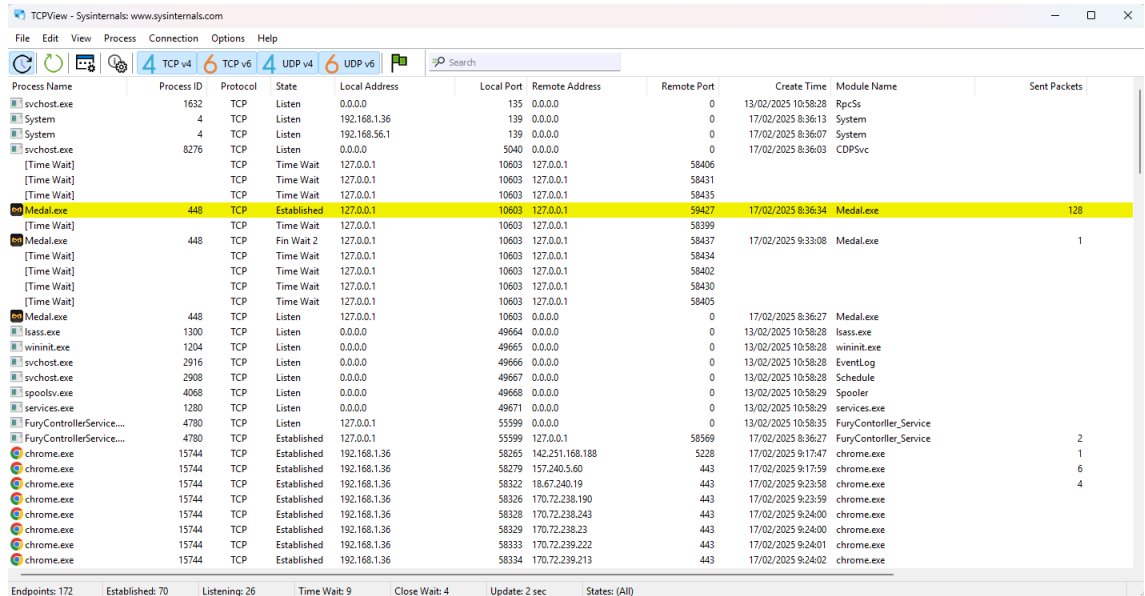
Parte 1 y parte 2

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1632	TCP	Listen	0.0.0.0	135	0.0.0.0	0	13/02/2025 10:58:28	RpcSs	
System	4	TCP	Listen	192.168.1.36	139	0.0.0.0	0	17/02/2025 8:36:13	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	17/02/2025 8:36:07	System	
svchost.exe	8276	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	17/02/2025 8:36:03	CDPSvc	
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58406			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58431			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58435			
Medal.exe	448	TCP	Established	127.0.0.1	10603	127.0.0.1	58427	17/02/2025 8:36:34	Medal.exe	128
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58399			
Medal.exe	448	TCP	Fin Wait 2	127.0.0.1	10603	127.0.0.1	58437	17/02/2025 9:33:08	Medal.exe	1
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58434			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58402			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58430			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58405			
Medal.exe	448	TCP	Listen	127.0.0.1	10603	0.0.0.0	0	17/02/2025 8:36:27	Medal.exe	
lsass.exe	1300	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	13/02/2025 10:58:28	lsass.exe	
wininit.exe	1204	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	13/02/2025 10:58:28	wininit.exe	
svchost.exe	2916	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	13/02/2025 10:58:28	Eventlog	
svchost.exe	2908	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	13/02/2025 10:58:28	Schedule	
spoolsv.exe	4068	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	13/02/2025 10:58:29	Spooler	
services.exe	1280	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	13/02/2025 10:58:29	services.exe	
FuryControllerService...	4780	TCP	Listen	127.0.0.1	55599	0.0.0.0	0	13/02/2025 10:58:35	FuryController_Service	
FuryControllerService...	4780	TCP	Established	127.0.0.1	55599	127.0.0.1	58569	17/02/2025 8:36:27	FuryController_Service	2
chrome.exe	15744	TCP	Established	192.168.1.36	58265	142.251.168.188	5228	17/02/2025 9:17:47	chrome.exe	1
chrome.exe	15744	TCP	Established	192.168.1.36	58279	157.240.5.60	443	17/02/2025 9:17:59	chrome.exe	6
chrome.exe	15744	TCP	Established	192.168.1.36	58322	18.67.240.19	443	17/02/2025 9:23:58	chrome.exe	4
chrome.exe	15744	TCP	Established	192.168.1.36	58326	170.72.238.190	443	17/02/2025 9:23:59	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58328	170.72.238.243	443	17/02/2025 9:24:00	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58329	170.72.238.23	443	17/02/2025 9:24:00	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58333	170.72.239.222	443	17/02/2025 9:24:01	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58334	170.72.239.213	443	17/02/2025 9:24:02	chrome.exe	

Endpoints: 172 Established: 70 Listening: 26 Time Wait: 9 Close Wait: 4 Update: 2 sec States: (All)

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.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1632	TCP	Listen	0.0.0.0	135	0.0.0.0	0	13/02/2025 10:58:28	RpcSs	
System	4	TCP	Listen	192.168.1.36	139	0.0.0.0	0	17/02/2025 8:36:13	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	17/02/2025 8:36:07	System	
svchost.exe	8276	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	17/02/2025 8:36:03	CDPSvc	
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58406			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58431			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58435			
Medal.exe	448	TCP	Established	127.0.0.1	10603	127.0.0.1	58427	17/02/2025 8:36:34	Medal.exe	128
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58399			
Medal.exe	448	TCP	Fin Wait 2	127.0.0.1	10603	127.0.0.1	58437	17/02/2025 9:33:08	Medal.exe	1
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58434			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58402			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58430			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58405			
Medal.exe	448	TCP	Listen	127.0.0.1	10603	0.0.0.0	0	17/02/2025 8:36:27	Medal.exe	
lsass.exe	1300	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	13/02/2025 10:58:28	lsass.exe	
wininit.exe	1204	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	13/02/2025 10:58:28	wininit.exe	
svchost.exe	2916	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	13/02/2025 10:58:28	EventLog	
svchost.exe	2908	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	13/02/2025 10:58:28	Schedule	
spoolsv.exe	4068	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	13/02/2025 10:58:29	Spooler	
services.exe	1280	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	13/02/2025 10:58:29	services.exe	
FuryControllerService....	4780	TCP	Listen	127.0.0.1	55599	0.0.0.0	0	13/02/2025 10:58:35	FuryController_Service	
FuryControllerService....	4780	TCP	Established	127.0.0.1	55599	127.0.0.1	58569	17/02/2025 8:36:27	FuryController_Service	2
chrome.exe	15744	TCP	Established	192.168.1.36	58265	142.251.168.188	5228	17/02/2025 9:17:47	chrome.exe	1
chrome.exe	15744	TCP	Established	192.168.1.36	58279	157.240.5.60	443	17/02/2025 9:17:59	chrome.exe	6
chrome.exe	15744	TCP	Established	192.168.1.36	58322	18.67.240.19	443	17/02/2025 9:23:58	chrome.exe	4
chrome.exe	15744	TCP	Established	192.168.1.36	58326	170.72.238.190	443	17/02/2025 9:23:59	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58328	170.72.238.243	443	17/02/2025 9:24:00	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58329	170.72.238.23	443	17/02/2025 9:24:00	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58333	170.72.239.222	443	17/02/2025 9:24:01	chrome.exe	
chrome.exe	15744	TCP	Established	192.168.1.36	58334	170.72.239.213	443	17/02/2025 9:24:02	chrome.exe	

Endpoints: 172 Established: 70 Listening: 26 Time Wait: 9 Close Wait: 4 Update: 2 sec States: (All)

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

El Servicio de Subsistema de Autoridad de Seguridad Local es un proceso en los sistemas operativos Microsoft Windows, responsable de hacer cumplir la política de seguridad en el sistema.

Ubicado en: **C:\Windows\System32\lsass.exe**

- a) Cierren la ventana de propiedades correspondiente a lsass.exe cuando hayan terminado
- b) 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.

Por ejemplo wininit.exe, es un proceso esencial de Windows, que desempeña un papel crucial tanto en el arranque como en el apagado del sistema operativo Windows

Ubicado en **C:\Windows\System32\wininit.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?

Los procesos que inician el navegador se ponen de color verde, indicando que se ha abierto el programa.

svchost.exe	2300	UDPv6	::	5555	^	11/02/2025 8:51:38	Unscache
msedge.exe	21912	UDPv6	::	5353	*	17/02/2025 9:44:01	msedge.exe
msedge.exe	21912	UDPv6	::	5353	*	17/02/2025 9:44:01	msedge.exe

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

Se vuelve de color rojo mientras se cierra el programa

msedge.exe	23700	TCP	Established	192.168.1.36	58719	52.236.29.249	443	17/02/2025 9:45:45	msedge.exe	5
msedge.exe	23700	TCP	Established	192.168.1.36	58720	52.98.250.162	443	17/02/2025 9:45:45	msedge.exe	3
svchost.exe	2500	UDP		0.0.0.0	49297	*		17/02/2025 9:43:58	DnsCache	
svchost.exe	2500	UDPv6		::	49297	*		17/02/2025 9:43:58	DnsCache	
msedge.exe	23700	TCP	Established	192.168.1.36	58723	13.74.129.1	443	17/02/2025 9:45:45	msedge.exe	5
msedge.exe	23700	TCP	Established	192.168.1.36	58727	13.88.179.11	443	17/02/2025 9:45:45	msedge.exe	21
SearchHost.exe	19480	TCP	Established	192.168.1.36	58599	204.79.197.222	443	17/02/2025 9:43:00	SearchHost.exe	7
SearchHost.exe	19480	TCP	Established	192.168.1.36	58624	150.171.23.12	443	17/02/2025 9:43:40	SearchHost.exe	6
msedge.exe	23700	UDP		0.0.0.0	51965	*		17/02/2025 9:45:34	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	58373	*		17/02/2025 9:45:34	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	58614	*		17/02/2025 9:45:34	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	58862	*		17/02/2025 9:45:45	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	58776	*		17/02/2025 9:45:33	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	60376	*		17/02/2025 9:45:45	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	63760	*		17/02/2025 9:45:45	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	64695	*		17/02/2025 9:45:34	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	50423	*		17/02/2025 9:45:45	msedge.exe	
msedge.exe	23700	TCP	Established	192.168.1.36	58716	2.21.34.16	443	17/02/2025 9:45:36	msedge.exe	3
msedge.exe	23700	TCP	Established	192.168.1.36	58710	131.253.33.203	443	17/02/2025 9:45:45	msedge.exe	6
msedge.exe	23700	TCP	Established	192.168.1.36	58724	150.171.28.10	443	17/02/2025 9:45:45	msedge.exe	3
msedge.exe	23700	TCP	Established	192.168.1.36	58725	131.253.33.203	443	17/02/2025 9:45:45	msedge.exe	3
msedge.exe	23700	TCP	Established	192.168.1.36	58726	108.157.98.10	443	17/02/2025 9:45:45	msedge.exe	2
msedge.exe	23700	UDP		0.0.0.0	56587	*		17/02/2025 9:45:45	msedge.exe	
msedge.exe	23700	UDP		0.0.0.0	57506	*		17/02/2025 9:45:45	msedge.exe	

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

msedge.exe	15260	TCP	Established	192.168.1.36	58767	13.107.246.77	443	17/02/2025 9:46:47	msedge.exe	
msedge.exe	15260	TCP	Established	192.168.1.36	58768	104.79.90.33	443	17/02/2025 9:46:47	msedge.exe	
msedge.exe	15260	TCP	Established	192.168.1.36	58769	204.79.197.239	443	17/02/2025 9:46:47	msedge.exe	
msedge.exe	15260	TCP	Established	192.168.1.36	58770	13.107.22.239	443	17/02/2025 9:46:47	msedge.exe	

Se quedan abiertas estas conexiones, puede ser a que haya procesos en segundo plano que las sigan ejecutando, que el cierre sea incompleto, o que alguno servicios de Microsoft como la sincronización o la actualización de datos en la nube, puede mantener activas las conexiones.



En el administrador de tareas podemos observar que está en segundo plano

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1632	TCP	Listen	0.0.0.0	135	0.0.0.0	0	13/02/2025 10:58:28	RpcSs	
System	4	TCP	Listen	192.168.1.36	139	0.0.0.0	0	17/02/2025 8:36:13	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	17/02/2025 8:36:07	System	
svchost.exe	8276	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	17/02/2025 8:36:03	CDPSvc	
Medal.exe	448	TCP	Listen	127.0.0.1	10603	0.0.0.0	0	17/02/2025 8:36:27	Medal.exe	
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58808			
Medal.exe	448	TCP	Fin Wait 2	127.0.0.1	10603	127.0.0.1	58822	17/02/2025 9:51:53	Medal.exe	
Medal.exe	448	TCP	Established	127.0.0.1	10603	127.0.0.1	59427	17/02/2025 8:36:34	Medal.exe	332
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58809			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58807			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58812			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58805			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58817			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58811			
[Time Wait]		TCP	Time Wait	127.0.0.1	10603	127.0.0.1	58821			
lsass.exe	1300	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	13/02/2025 10:58:28	lsass.exe	
wininit.exe	1204	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	13/02/2025 10:58:28	wininit.exe	
svchost.exe	2916	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	13/02/2025 10:58:28	EventLog	
svchost.exe	2908	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	13/02/2025 10:58:28	Schedule	
spoolsv.exe	4068	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	13/02/2025 10:58:29	Spooler	
services.exe	1280	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	13/02/2025 10:58:29	services.exe	
FuryControllerService....	4780	TCP	Listen	127.0.0.1	55599	0.0.0.0	0	13/02/2025 10:58:35	FuryController_Service	
FuryControllerService....	4780	TCP	Established	127.0.0.1	55599	127.0.0.1	58569	17/02/2025 8:36:27	FuryController_Service	6
svchost.exe	4708	TCP	Established	192.168.1.36	58447	4.207.247.139	443	17/02/2025 8:36:09	WpnService	1
OneDrive.exe	9228	TCP	Established	192.168.1.36	58473	4.207.247.139	443	17/02/2025 8:36:15	OneDrive.exe	7
EpicGamesLauncher.e...	15688	TCP	Established	192.168.1.36	58480	52.86.153.4	443	17/02/2025 8:36:16	EpicGamesLauncher.exe	9
RiotClientServices.exe	7844	TCP	Close Wait	192.168.1.36	58503	172.64.146.73	443	17/02/2025 8:36:18	RiotClientServices.exe	
RiotClientServices.exe	7844	TCP	Close Wait	192.168.1.36	58506	172.64.146.73	443	17/02/2025 8:36:18	RiotClientServices.exe	
RiotClientServices.exe	7844	TCP	Listen	127.0.0.1	58513	0.0.0.0	0	17/02/2025 8:36:19	RiotClientServices.exe	
Medal.exe	8004	TCP	Established	192.168.1.36	58561	15.197.213.252	443	17/02/2025 8:36:27	Medal.exe	4
FURYCTRL.exe	14612	TCP	Established	127.0.0.1	58569	127.0.0.1	55599	17/02/2025 8:36:27	FURYCTRL.exe	6

Una vez cerrado a la fuerza, desaparecen las conexiones