

Class Activity – Identify Running Processes

Objectives

In this lab, you will use TCP/UDP Endpoint Viewer, a tool in Sysinternals Suite, to identify any running processes on your computer.

Background / Scenario

In this lab, you will explore processes. Processes are programs or applications in execution. You will explore the processes using Process Explorer in the Windows Sysinternals Suite. You will also start and observe a new process.

Required Resources

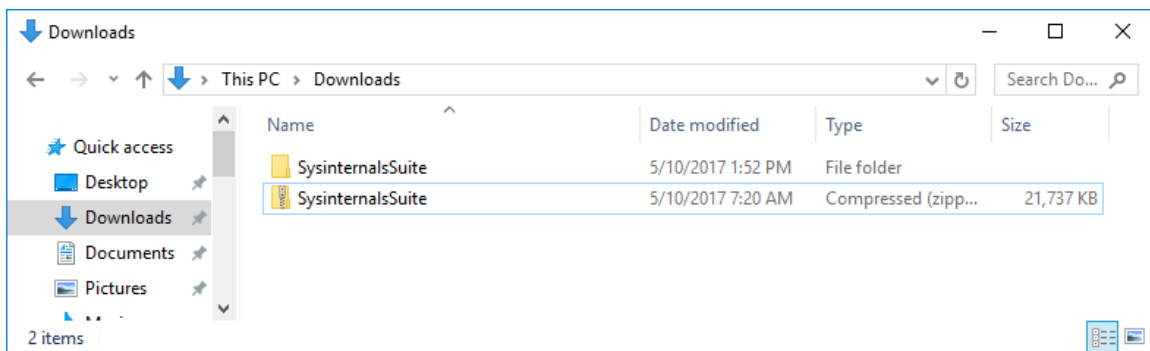
- 1 Windows PC with Internet access

Step 1: Download Windows Sysinternals Suite.

- Navigate to the following link to download Windows Sysinternals Suite:
<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- After the download is completed, right-click the zip file, and choose **Extract All...**, to extract the files from the folder. Choose the default name and destination in the Downloads folder and click **Extract**.
- Exit the web browser.

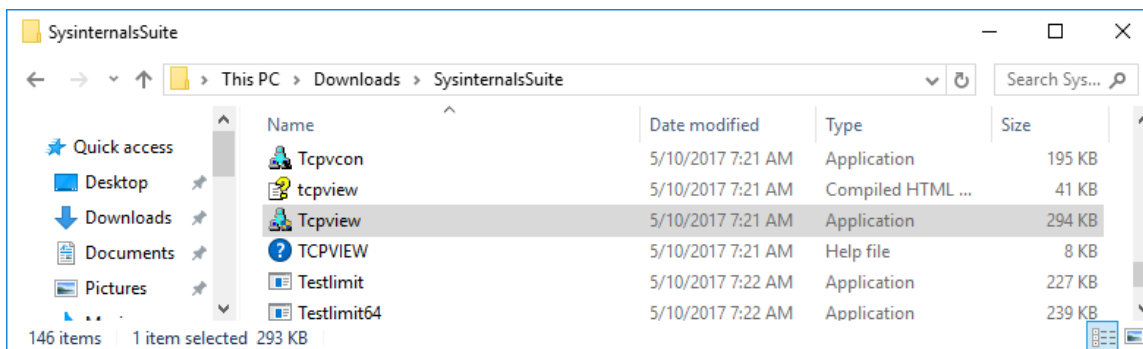
Step 2: Start TCP/UDP Endpoint Viewer.

- Navigate to the SysinternalsSuite folder with all the extracted files.



Class Activity – Identify Running Processes

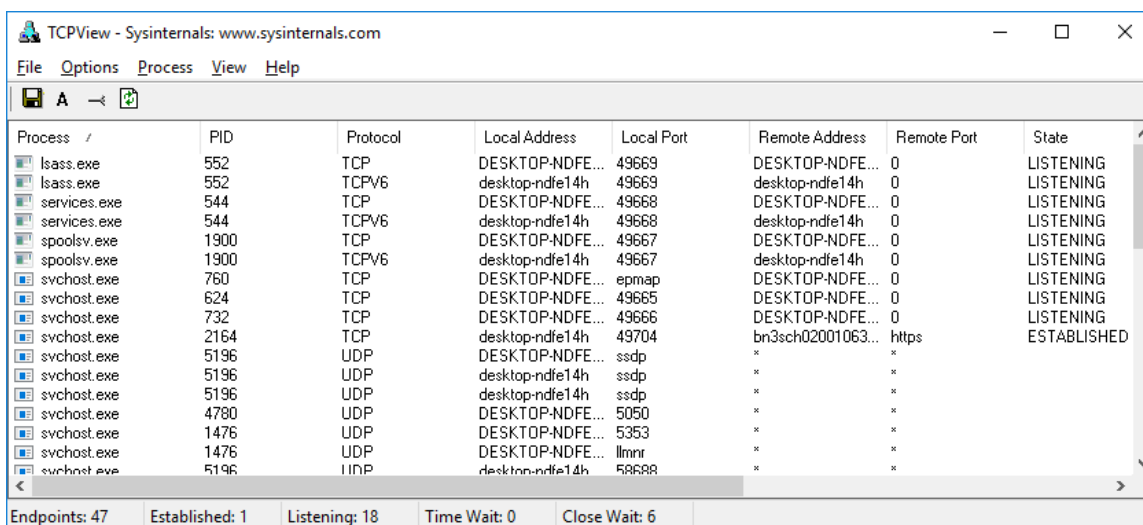
- b. Open **Tcpview.exe**. Accept the Process Explorer License Agreement when prompted. Click **Yes** to allow this app to make changes to your device.



- c. Exit the File Explorer and close all the currently running applications.

Step 3: Explore the running processes.

- a. TCPView lists the process that are currently on your Windows PC. At this time, only Windows processes are running.



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
services.exe	544	TCP	DESKTOP-NDFE...	49668	DESKTOP-NDFE...	0	LISTENING
services.exe	544	TCPV6	desktop-ndfe14h	49668	desktop-ndfe14h	0	LISTENING
spoolsv.exe	1900	TCP	DESKTOP-NDFE...	49667	DESKTOP-NDFE...	0	LISTENING
spoolsv.exe	1900	TCPV6	desktop-ndfe14h	49667	desktop-ndfe14h	0	LISTENING
svchost.exe	760	TCP	DESKTOP-NDFE...	epmap	DESKTOP-NDFE...	0	LISTENING
svchost.exe	624	TCP	DESKTOP-NDFE...	49665	DESKTOP-NDFE...	0	LISTENING
svchost.exe	732	TCP	DESKTOP-NDFE...	49666	DESKTOP-NDFE...	0	LISTENING
svchost.exe	2164	TCP	desktop-ndfe14h	49704	bn3sch02001063...	https	ESTABLISHED
svchost.exe	5196	UDP	DESKTOP-NDFE...	ssdp	*	*	
svchost.exe	5196	UDP	desktop-ndfe14h	ssdp	*	*	
svchost.exe	5196	UDP	desktop-ndfe14h	ssdp	*	*	
svchost.exe	4780	UDP	DESKTOP-NDFE...	5050	*	*	
svchost.exe	1476	UDP	DESKTOP-NDFE...	5353	*	*	
svchost.exe	1476	UDP	DESKTOP-NDFE...	llmnr	*	*	
svchost.exe	5196	UDP	desktop-ndfe14h	58588	*	*	

- b. Double-click **lsass.exe**.

What is lsass.exe? In what folder is it located?

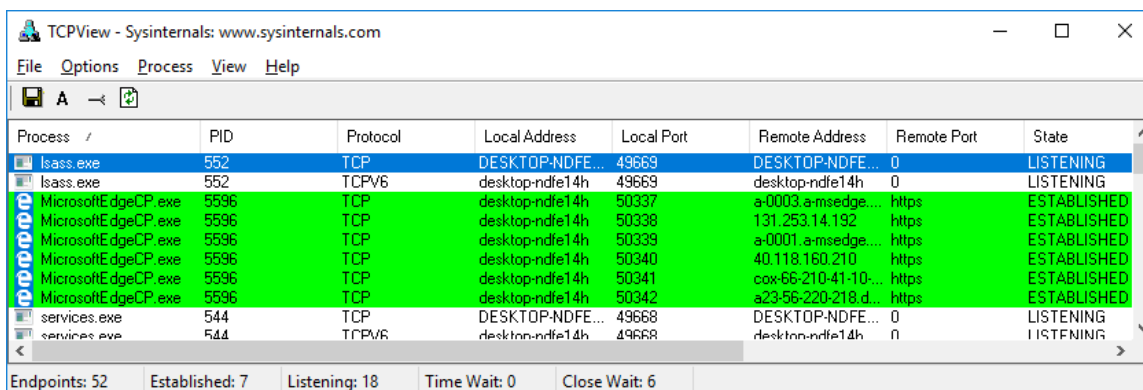
- c. Close the properties window for lsass.exe when done.
d. View the properties for the other running processes.

Note: Not all processes can be queried for properties information.

Step 4: Explore a user-started process.

- Open a web browser, such as Microsoft Edge.

What did you observe in the TCPView window?



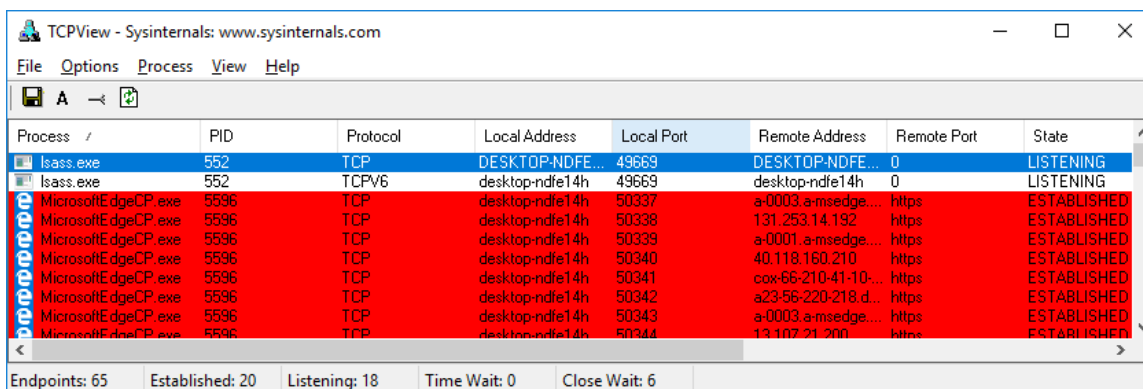
The screenshot shows the TCPView application window. The process list on the left includes lsass.exe (PID 552) and MicrosoftEdgeCP.exe (PID 5596). The main table displays network connections. lsass.exe is listening on port 49669. MicrosoftEdgeCP.exe has several established connections on ports 50337 through 50342. 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

- Close the web browser.

What did you observe in the TCPView window?



The screenshot shows the TCPView application window after the web browser has been closed. The process list on the left includes lsass.exe (PID 552) and MicrosoftEdgeCP.exe (PID 5596). The main table displays network connections. lsass.exe is still listening on port 49669. MicrosoftEdgeCP.exe now has 10 established connections on ports 50337 through 50344. 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
services.exe	544	TCP	DESKTOP-NDFE...	49668	DESKTOP-NDFE...	0	LISTENING
services.exe	544	TCPV6	desktop-ndfe14h	49668	desktop-ndfe14h	0	LISTENING

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

- Reopen the web browser. Research some of the processes listed in TCPView. Record your findings.
