



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.

Part 1: Download Windows Sysinternals Suite.

Part 2: Start TCP/UDP Endpoint Viewer.

Part 3: Explore the running processes.

Part 4: Explore a user-started process.

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

Instructions

Part 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.

Part 2: Start TCP/UDP Endpoint Viewer.

- Navigate to the SysinternalsSuite folder with all the extracted files.
- Open **Tcpview.exe**. Accept the Process Explorer License Agreement when prompted. Click **Yes** to allow this app to make changes to your device.
- Exit the File Explorer and close all the currently running applications.

Part 3: Explore the running processes.

- TCPView lists the process that are currently on your Windows PC. At this time, only Windows processes are running.
- Double-click **lsass.exe**.
What is lsass.exe? In what folder is it located? **Path: C:\Windows\System32\lsass.exe**
lsass.exe stands for Local Security Authority Subsystem Service. It is an essential process in the Windows operating system responsible for several security-related functions.
- Close the properties window for lsass.exe when done.

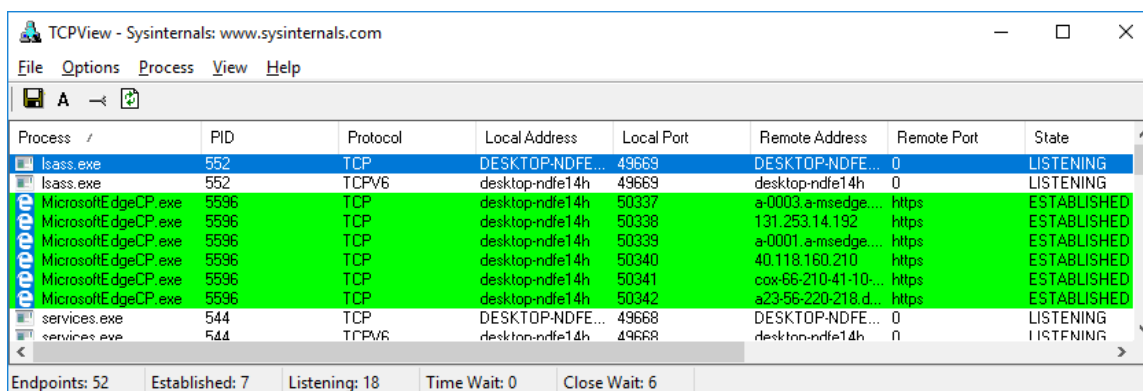
- d. View the properties for the other running processes.

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

Part 4: Explore a user-started process.

- a. Open a web browser, such as Microsoft Edge.

What did you observe in the TCPView window?



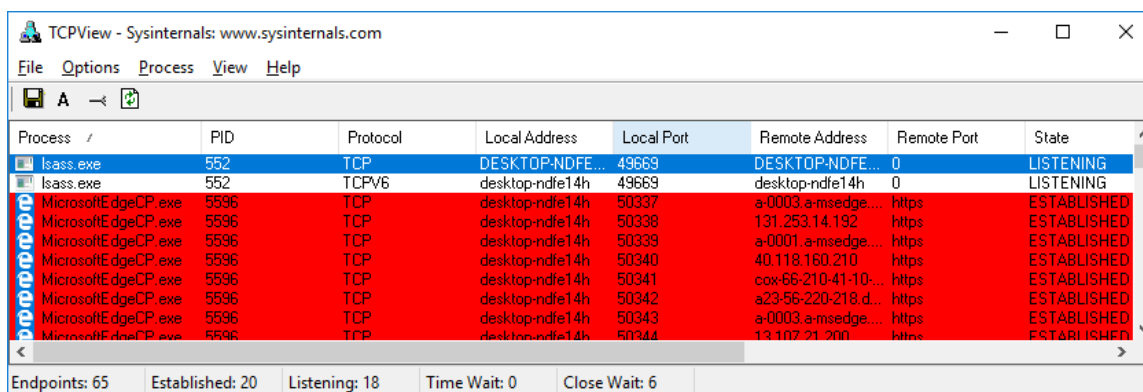
The screenshot shows the TCPView application window. The table lists the following connections:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
Isass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
Isass.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

Summary statistics at the bottom: Endpoints: 52, Established: 7, Listening: 18, Time Wait: 0, Close Wait: 6.

- b. 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 table lists the following connections:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
Isass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
Isass.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

Summary statistics at the bottom: Endpoints: 65, Established: 20, Listening: 18, Time Wait: 0, Close Wait: 6.

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

System: This process represents various system-level operations and services.

wininit.exe: a legitimate Windows system process that plays a crucial role during system startup.

svchost.exe: a crucial Windows system process responsible for hosting multiple Windows services. It's essential for the functioning of various system services, and multiple instances may run simultaneously.

spoolsv.exe: a Windows system process responsible for managing print spooler services. It handles print jobs sent to the printer and ensures they are processed in the correct order.

services.exe: a critical system process in Windows responsible for managing system services. It starts, stops, and interacts with Windows services, which are background processes responsible for various system functions and tasks.