Class Activity - Identify Running Processes (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# 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

## Download Windows Sysinternals Suite.

* + 1. Navigate to the following link to download Windows Sysinternals Suite:

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

* + 1. 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**.
    2. Exit the web browser.

## Start TCP/UDP Endpoint Viewer.

* + 1. Navigate to the SysinternalsSuite folder with all the extracted files.
    2. Open **Tcpview.exe**. Accept the Process Explorer License Agreement when prompted. Click **Yes** to allow this app to make changes to your device.
    3. Exit the File Explorer and close all the currently running applications.

## Explore the running processes.

* + 1. TCPView lists the process that are currently on your Windows PC. At this time, only Windows processes are running.
    2. Double-click **lsass.exe**.

### Question:

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

Type your answers here.

Local Security Authority Process is the name for lsass.exe. It is located in C:\Windows\System32\ folder.

* + 1. Close the properties window for lsass.exe when done.
    2. View the properties for the other running processes.

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

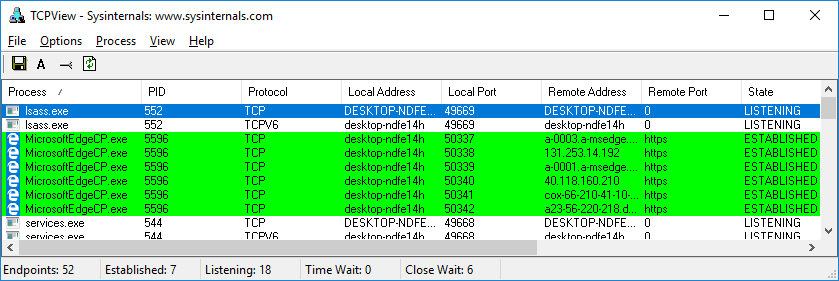
## Explore a user-started process.

* + 1. Open a web browser, such as Microsoft Edge.

What did you observe in the TCPView window?

Type your answers here.

The processes for the web browser are added to the TCPView window.



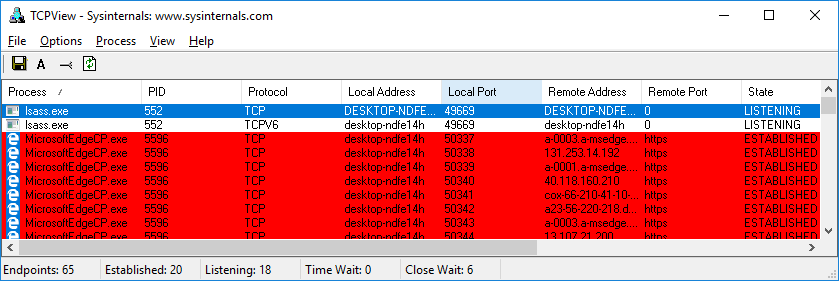
* + 1. Close the web browser.

### Question:

What did you observe in the TCPView window?

Type your answers here.

The processes for the web browser will be removed from the TCPView window.



* + 1. Reopen the web browser. Research some of the processes listed in TCPView. Record your findings.

Type your answers here.

Answers will vary. The process lsass.exe verifies the validity of user logins to the PC. The services.exe is used to start and stop services and change the default services startup settings. The process svnhost.exe (Service Host) handles the process of sharing system resources. Most of these listed resources are located in the C:\Windows\System32\ folder. If these executables are found elsewhere in the system, they maybe malware, such as viruses, spyware, trojans or worms.

End of document