



Lab 2.0.1.2 – Identify Running Processes



This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

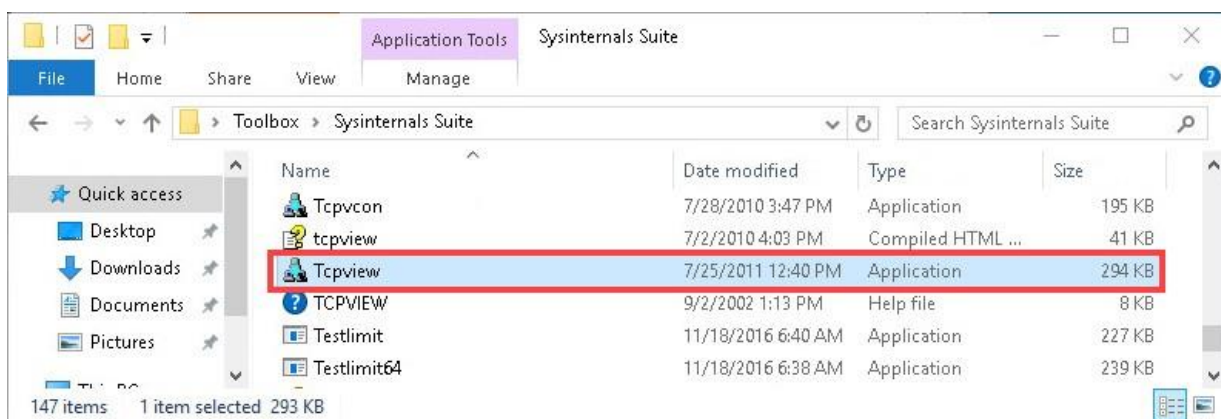
In this lab, you will use TCP/UDP Endpoint Viewer, a tool in Sysinternals Suite, to identify any running processes on your computer.

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.

Step 1: Start TCP/UDP Endpoint Viewer.

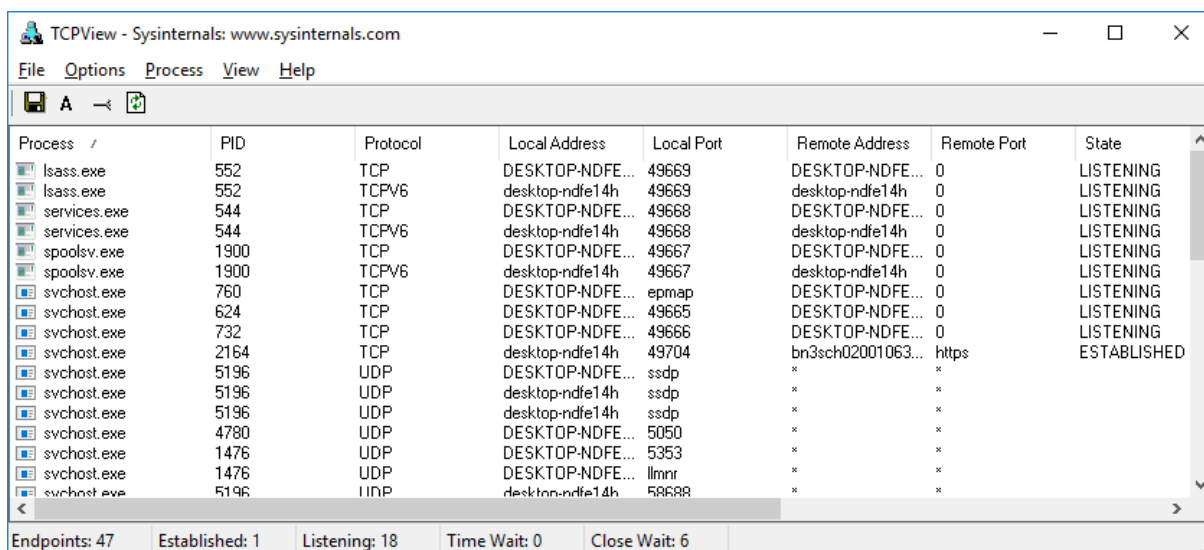
- Access the **WinClient** machine. Unlock the machine by clicking on the drop-down arrow for that specific machine's tab and select **Send CTRL+ALT+DEL**.
- Login as the administrator using cyberops as the password.
- Navigate to the **Toolbox** folder located on the *Desktop* and then double-click the **Sysinternals Suite** folder.
- Locate and double-click the **Tcpview.exe** application file. Accept the *Process Explorer License Agreement* when prompted. If prompted, click **Yes** to allow this app to make changes to your device.



- Exit the **File Explorer** and close all the currently running applications. Leave the *TCPView* application open.

Step 2: Explore the running processes.

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



The screenshot shows the TCPView application window with the following data:

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	58688	*	*	

Endpoints: 47 Established: 1 Listening: 18 Time Wait: 0 Close Wait: 6

- b. Double-click either instance of **lsass.exe**.

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

lsass.exe is an Local Security Authority Subsystem Service it is a window process which takes responsibility of Security for the operating System.

C:\Windows\System32\lsass.exe

- c. Click **OK** to 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. For example, double-click on one of the System processes.

Step 3: Explore a user-started process.

- a. Open the **Mozilla Firefox** web browser.

What did you observe in the *TCPView* window?

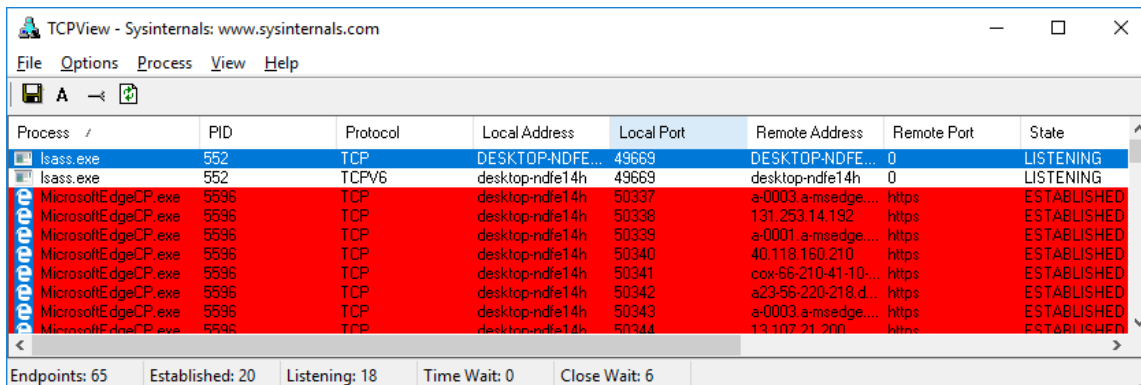
When I opened Mozilla Firefox in web browser, I can see that some more new process of firefox.exe is added in TCP view window.

Lab - Identify Running Processes

- b. Close the web browser.

What did you observe in the TCPView window?

When I closed the web browser, I can see that no past process is running everything is removed from the TCP view window.



The screenshot shows the TCPView application window from Sysinternals. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu is a toolbar with icons for saving, refreshing, and zooming. The main area is a table of network connections. The table has columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The first two rows show 'lsass.exe' with PID 552, listening on port 49669. The subsequent rows show 'MicrosoftEdgeCP.exe' with PID 5596, with various established connections to different remote addresses and ports. The bottom status bar shows statistics: Endpoints: 65, Established: 20, Listening: 18, Time Wait: 0, Close Wait: 6.

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

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.

When I reopened the Firefox, the process was added to in the TCP view window

With the similar Local Address and state was established. Some processes are changing with red and green. Changing of colours and state establishment.