3.0.3 Lab - 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 Windows Sysinternals Suite used to identify any running processes on your computer.

Part 1: Start TCP/UDP Endpoint Viewer.

Part 2: Explore the running processes.

Part 3: 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.

Instructions

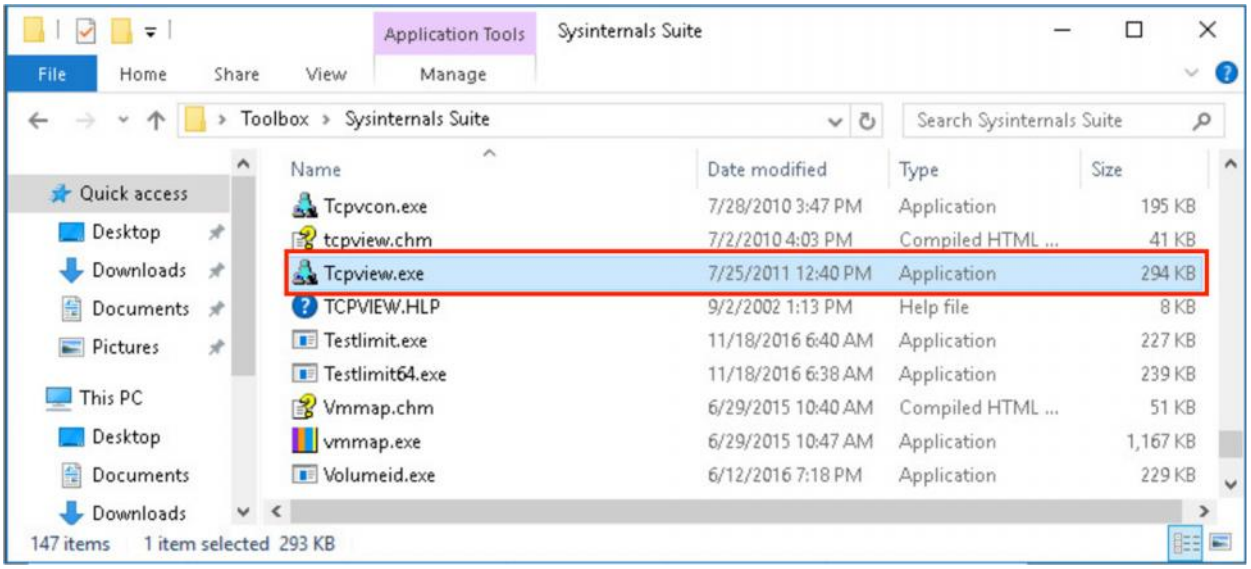
Part 1: Start TCP/UDP Endpoint Viewer.

a. 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**.

b. Login as the `Administrator` using `cyberops` as the password.

c. Navigate to the **Toolbox** folder located on the Desktop and then double-click the **Sysinternals Suite** folder.

d. Locate and double-click the **Tcpview.exe** application file. Accept the *TCPView License Agreement* when prompted. If prompted, click **Yes** to allow this app to make changes to your device.



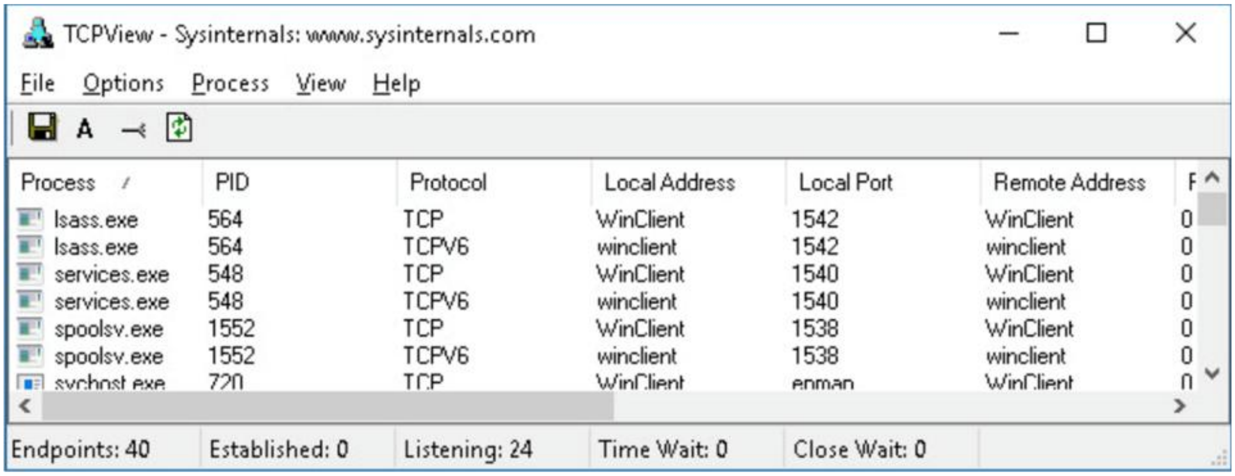
Name	Date modified	Type	Size
Tcpvcon.exe	7/28/2010 3:47 PM	Application	195 KB
tcpview.chm	7/2/2010 4:03 PM	Compiled HTML ...	41 KB
Tcpview.exe	7/25/2011 12:40 PM	Application	294 KB
TCPVIEW.HLP	9/2/2002 1:13 PM	Help file	8 KB
Testlimit.exe	11/18/2016 6:40 AM	Application	227 KB
Testlimit64.exe	11/18/2016 6:38 AM	Application	239 KB
Vmmap.chm	6/29/2015 10:40 AM	Compiled HTML ...	51 KB
vmmap.exe	6/29/2015 10:47 AM	Application	1,167 KB
Volumeid.exe	6/12/2016 7:18 PM	Application	229 KB

147 items 1 item selected 293 KB

e. Exit the **File Explorer** application. Leave the *TCPView* application open.

Part 2: 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	F
lsass.exe	564	TCP	WinClient	1542	WinClient	0
lsass.exe	564	TCPV6	winclient	1542	winclient	0
services.exe	548	TCP	WinClient	1540	WinClient	0
services.exe	548	TCPV6	winclient	1540	winclient	0
spoolsv.exe	1552	TCP	WinClient	1538	WinClient	0
spoolsv.exe	1552	TCPV6	winclient	1538	winclient	0
svchost.exe	720	TCP	WinClient	epmap	WinClient	0

Endpoints: 40 Established: 0 Listening: 24 Time Wait: 0 Close Wait: 0

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

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

____

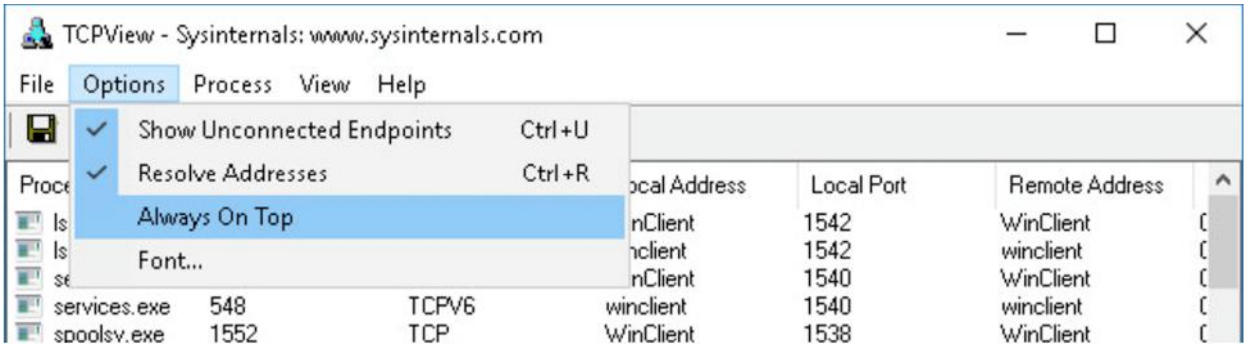
c. Click **OK** to close the properties window for lsass.exe when done.

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.

Part 3: Explore a user-started process.

a. In the TCPView window, click the **Options** dropdown menu, check **Always On Top** option.

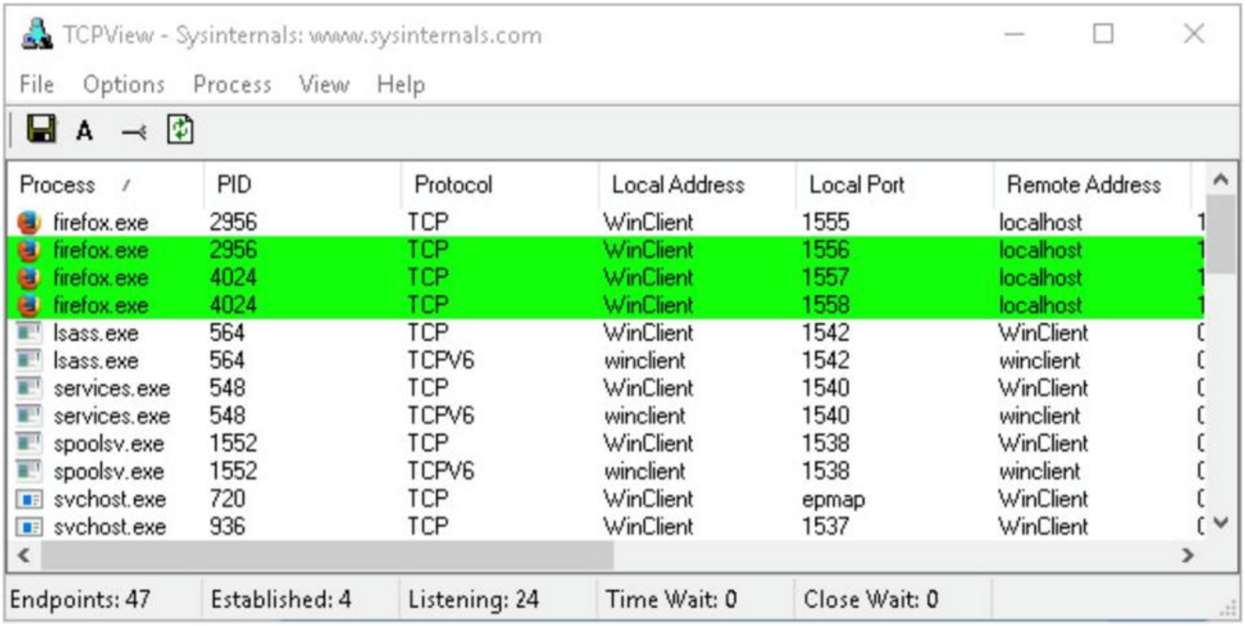

TCPView - Sysinternals: www.sysinternals.com
File
Options
Process
View
Help
✓ Show Unconnected Endpoints Ctrl+U
✓ Resolve Addresses Ctrl+R
Always On Top
Font...

Proce			ocal Address	Local Port	Remote Address	
ls			nClient	1542	WinClient	(
ls			nclient	1542	winclient	(
se			nClient	1540	WinClient	(
services.exe	548	TCPV6	winclient	1540	winclient	(
spoolsv.exe	1552	TCP	WinClient	1538	WinClient	(

b. Open the **Mozilla Firefox** web browser.

What did you observe in the TCPView window?

____



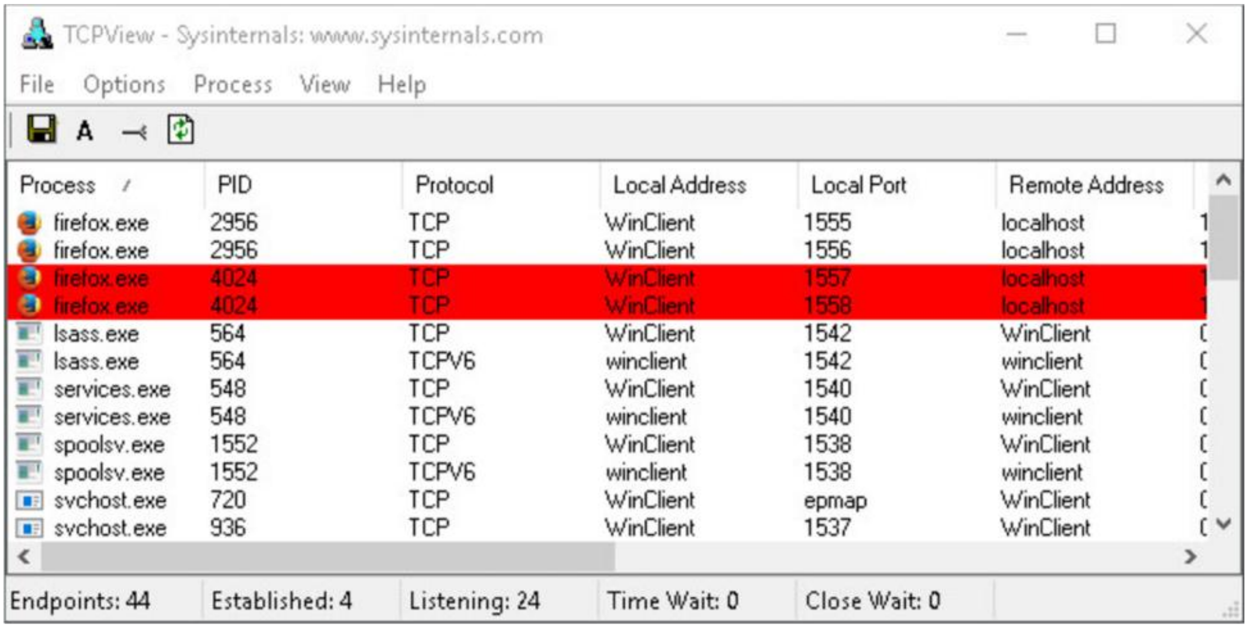
Process	PID	Protocol	Local Address	Local Port	Remote Address	
firefox.exe	2956	TCP	WinClient	1555	localhost	1
firefox.exe	2956	TCP	WinClient	1556	localhost	1
firefox.exe	4024	TCP	WinClient	1557	localhost	1
firefox.exe	4024	TCP	WinClient	1558	localhost	1
lsass.exe	564	TCP	WinClient	1542	WinClient	(
lsass.exe	564	TCPV6	winclient	1542	winclient	(
services.exe	548	TCP	WinClient	1540	WinClient	(
services.exe	548	TCPV6	winclient	1540	winclient	(
spoolsv.exe	1552	TCP	WinClient	1538	WinClient	(
spoolsv.exe	1552	TCPV6	winclient	1538	winclient	(
svchost.exe	720	TCP	WinClient	epmap	WinClient	(
svchost.exe	936	TCP	WinClient	1537	WinClient	(

Endpoints: 47 | Established: 4 | Listening: 24 | Time Wait: 0 | Close Wait: 0

c. Close the web browser.

What did you observe in the TCPView window?

____



Process	PID	Protocol	Local Address	Local Port	Remote Address
firefox.exe	2956	TCP	WinClient	1555	localhost
firefox.exe	2956	TCP	WinClient	1556	localhost
firefox.exe	4024	TCP	WinClient	1557	localhost
firefox.exe	4024	TCP	WinClient	1558	localhost
lsass.exe	564	TCP	WinClient	1542	WinClient
lsass.exe	564	TCPV6	winclient	1542	winclient
services.exe	548	TCP	WinClient	1540	WinClient
services.exe	548	TCPV6	winclient	1540	winclient
spoolsv.exe	1552	TCP	WinClient	1538	WinClient
spoolsv.exe	1552	TCPV6	winclient	1538	winclient
svchost.exe	720	TCP	WinClient	epmap	WinClient
svchost.exe	936	TCP	WinClient	1537	WinClient

Endpoints: 44 Established: 4 Listening: 24 Time Wait: 0 Close Wait: 0

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

____