

Class Activity - What's Going On?

Objectives

Identify the processes running on a computer, the protocol they are using, and their local and remote port addresses.

Part 1: Download and install the TCPView software.

Part 2: Answer the following questions.

Part 3: Use a browser and observe the TCPView window.

Background / Scenario

For a hacker to establish a connection to a remote computer, a port must be listening on that device. This may be due to infection by malware, or a vulnerability in a legitimate piece of software. A utility, such as TCPView, can be used to detect open ports, monitor them in real-time, and close active ports and processes using them.

Required Resources

- PC with Internet access
- TCPView software

Instructions

Part 1: Download and install the TCPView software.

- a. Click the link below to reach the download page for TCPView.

Class Activity - What's Going On?

<http://technet.microsoft.com/en-us/sysinternals/tcpview.aspx>

The screenshot shows the Windows Sysinternals TCPView v3.05 download page. The page includes a navigation bar with links to Home, Learn, Downloads, and Community. The main content area features the TCPView v3.05 download link, a 'Download TCPView (285 KB)' button, and a 'Run TcpView now from Live.Sysinternals.com' button. The page also includes a 'Share this content' section with social media links and an 'Introduction' section describing the tool. A small screenshot of the TCPView application interface is shown at the bottom.

- Create a folder on the desktop named **TCPView**.
- Extract the contents of the zip to this new folder.
- Start the Tcpview Application.
- Finally, Agree to the software license terms.

The screenshot shows the TCPView application interface. The window title is 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes File, Options, Process, View, and Help. The main display area shows a table of network connections with columns for Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Rcvd Packets, and Rcvd Bytes. The table lists various processes and their network activity, including listening ports and established connections. At the bottom, summary statistics are displayed: Endpoints: 55, Established: 1, Listening: 24, Time Wait: 0, Close Wait: 0.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
lsass.exe	476	TCP	pi	58702	pi	0	LISTENING				
lsass.exe	476	TCPv6	pi	58702	pi	0	LISTENING				
services.exe	468	TCP	pi	49155	pi	0	LISTENING				
services.exe	468	TCPv6	pi	49155	pi	0	LISTENING				
svchost.exe	716	TCP	pi	epmap	pi	0	LISTENING				
svchost.exe	768	TCP	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCP	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDP	pi.cisco.com	ssdp	*	*		36	17,142	462	91,080
svchost.exe	1408	UDP	pi	ssdp	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	972	UDP	pi	llmnr	*	*					
svchost.exe	972	UDP	pi	54649	*	*					
svchost.exe	1408	UDP	pi	61427	*	*					
svchost.exe	312	UDP	pi	61464	*	*					
svchost.exe	1408	UDP	pi.cisco.com	63677	*	*					
svchost.exe	1408	UDP	pi	63678	*	*					
svchost.exe	716	TCPv6	pi	epmap	pi	0	LISTENING				
svchost.exe	2300	TCPv6	pi	3587	pi	0	LISTENING				
svchost.exe	768	TCPv6	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCPv6	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDPv6	[0.0.0.0::0.1]	1900	*	*					
svchost.exe	1408	UDPM6	pi.cisco.com	1900	*	*					

Endpoints: 55 Established: 1 Listening: 24 Time Wait: 0 Close Wait: 0

Part 2: Answer the following questions.

- a. How many Endpoints are listed?
- b. How many are Listening?
- c. How many Endpoints are Established?

Part 3: Use a browser and observe the TCPView window.

- a. Open the Options menu and click "Always on Top".
Note: Use the Help section of the program to help you answer the following questions.
- b. Open any browser.

What happens in the TCPView window?

- c. Browse to cisco.com.

What happens in the TCPView window?

- d. Close the browser.

What happens in the TCPView window?

What do you think the colors mean?

Note: To close a process directly, right-click the process and choose **End Process**. Using this method can cause a program or the operating system to become unstable. Only end processes that you know are safe to end. This method can be used to stop malware from communicating.