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

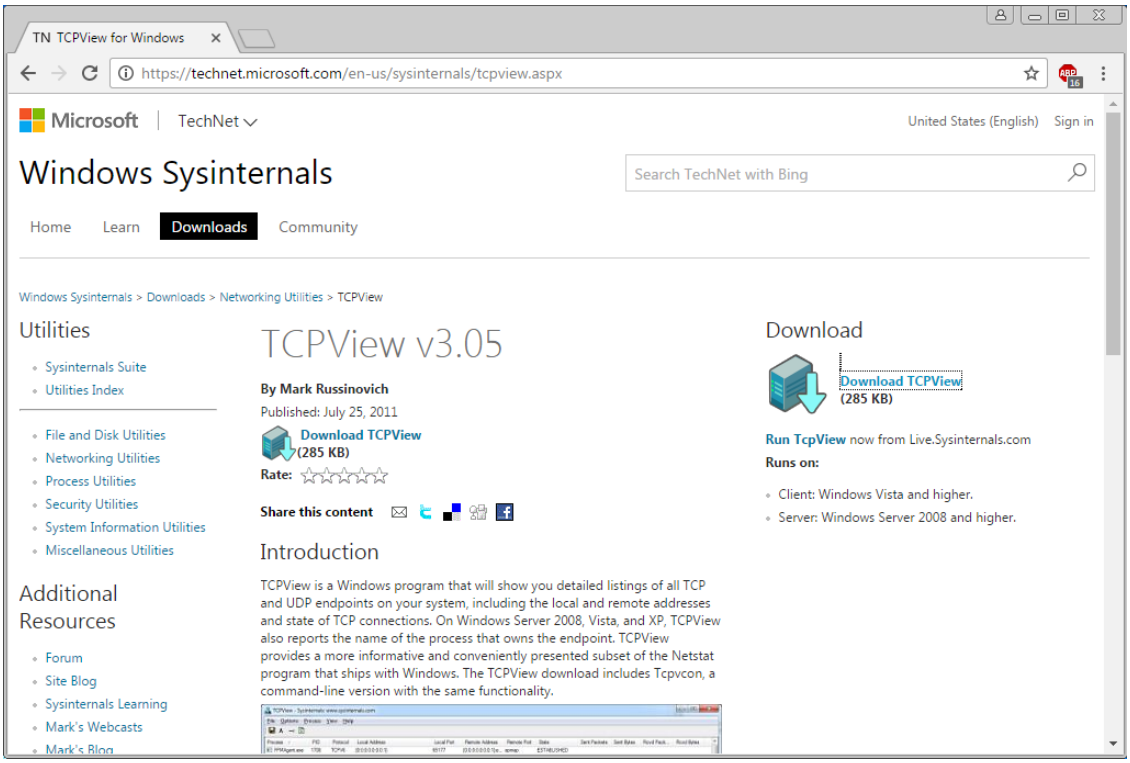
Instructions

Part 1: Download and install the TCPView software.

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

© 2017 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

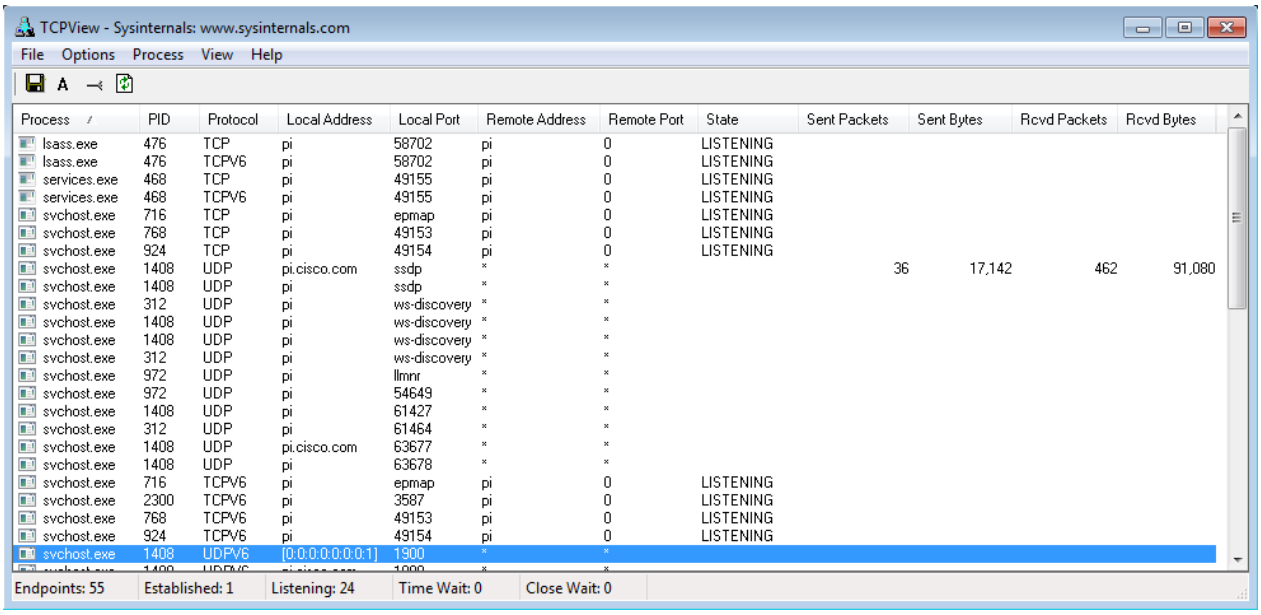


b. Create a folder on the desktop named **TCPView**.

c. Extract the contents of the zip to this new folder.

d. Start the Tcpview Application.

e. Finally, Agree to the software license terms.



© 2017 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2017 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public