

Đặng Hoàng Nguyên – SE171946

**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

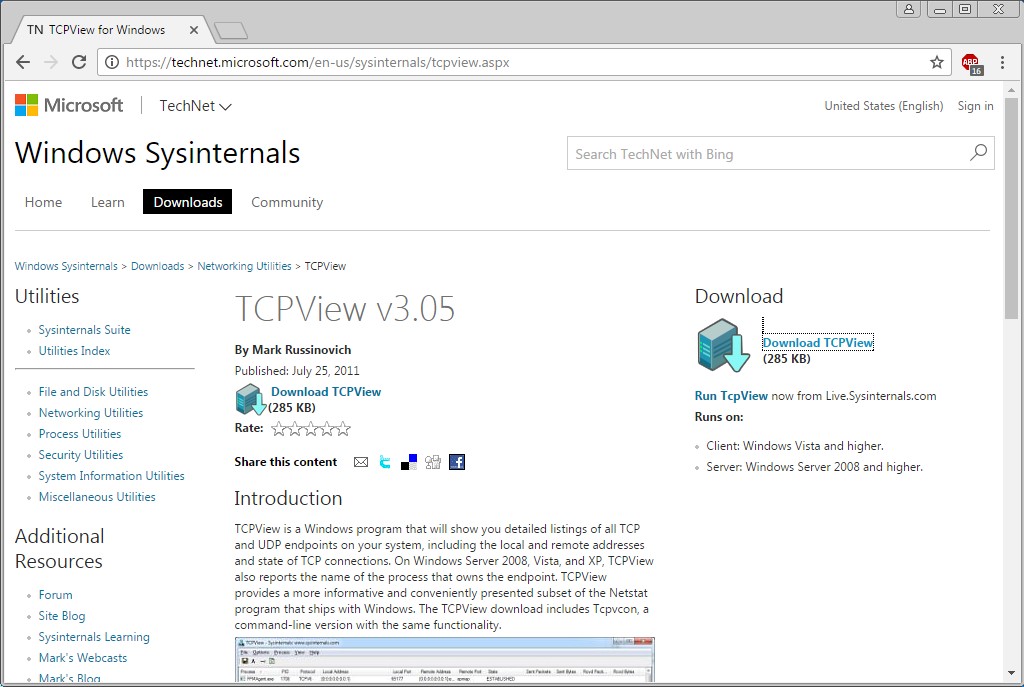
# Instructions

**Part 1: Download and install the TCPView software.**

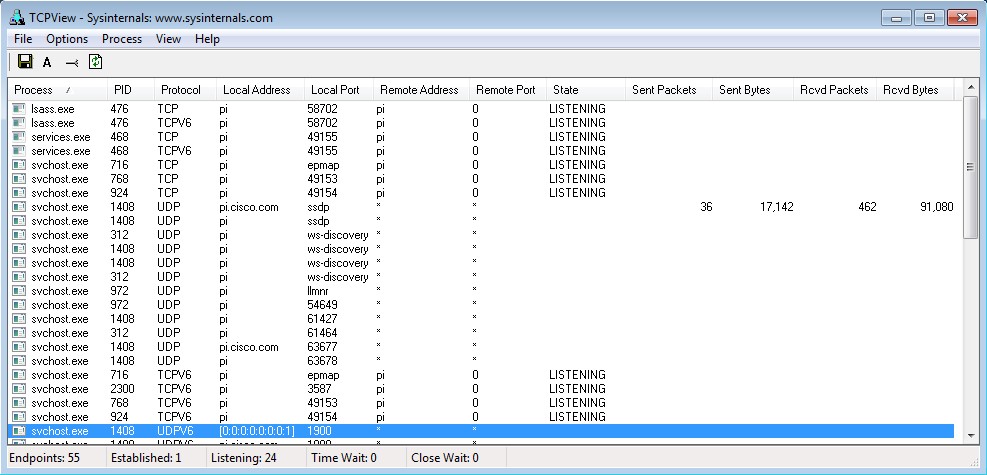
1. Click the link below to reach the download page for TCPView.

**Class Activity - What's Going On?**

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



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



**Class Activity - What's Going On?**

**Part 2: Answer the following questions.**

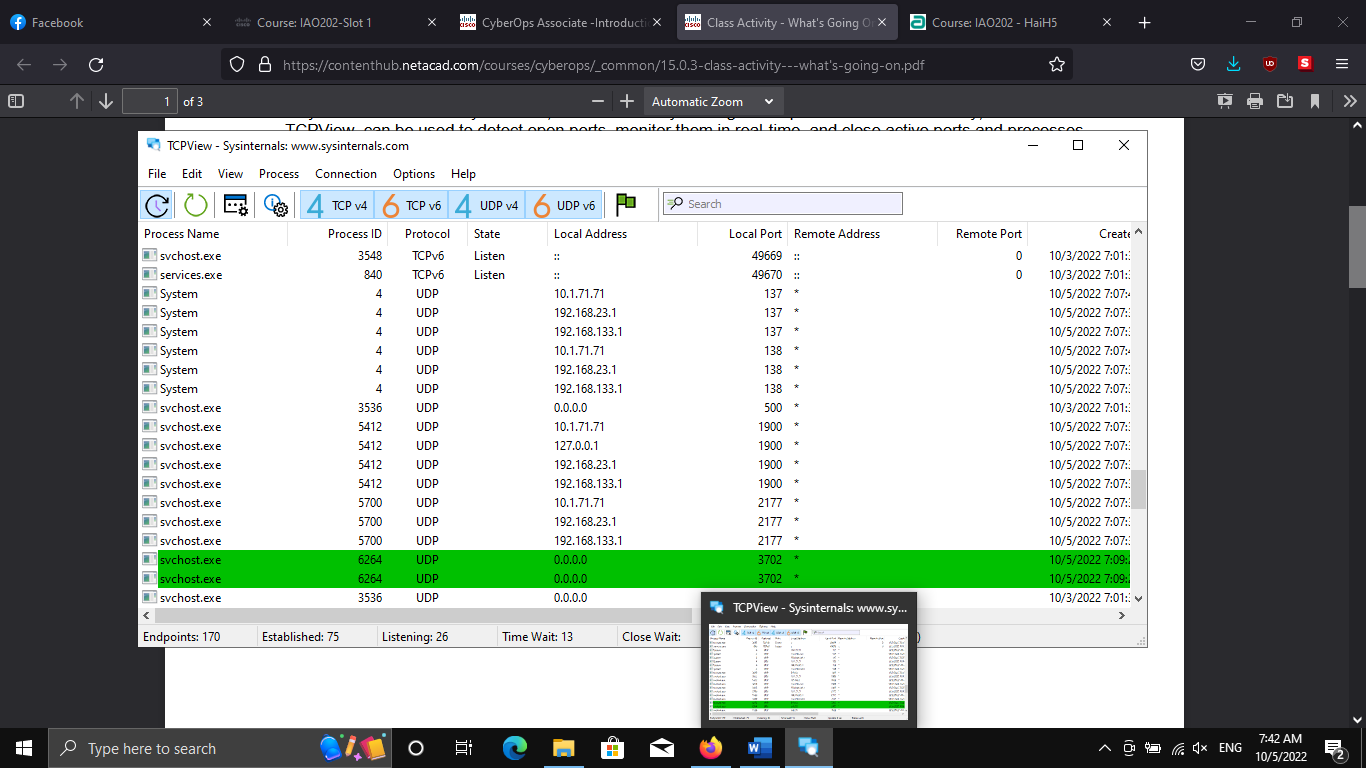
Questions:

1. How many Endpoints are listed?

***Type your answers here.***

1. How many are Listening?

There are 26 listening



1. How many Endpoints are Established?

There are 19 endpoints established

A screenshot of a computer

Description automatically generated

**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.

Question:

What happens in the TCPView window?

When opening a new browser, TCPView will appear at the bottom

1. Graphical user interface, application, table, Excel

   Description automatically generatedBrowse to cisco.com.

Question:

What happens in the TCPView window?

Graphical user interface

Description automatically generatedIt will appear at the bottom

1. Close the browser.

Questions:

What happens in the TCPView window?

The application turn to red

Graphical user interface, application, table, Excel

Description automatically generated

What do you think the colors mean?

Green – starting a process

White – process is running

Red – process is closing

**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.

*End of document*