Actividad de Clase - ¿Qué está sucediendo?
Objetivos

Identificar los procesos que se están ejecutando en una computadora, el protocolo que están utilizando y las direcciones de sus puertos locales y remotos.

Parte 1: Descargar e Instalar el software llamado TCPView.

Parte 2: Responder las siguientes preguntas.

Parte 3: Utilizar un navegador y observe la ventana de TCPView.

Aspectos básicos / Escenario

Para que un hacker pueda establecer una conexión a una computadora remota, un puerto debe estar escuchando en ese dispositivo. Esto puede deberse a infección de malware o a una vulnerabilidad en un componente de software legítimo. Se puede emplear una utilidad, como TCPView, para detectar puertos abiertos, monitorearlos en tiempo real y cerrar los puertos activos y los procesos que los están utilizando.

Recursos necesarios

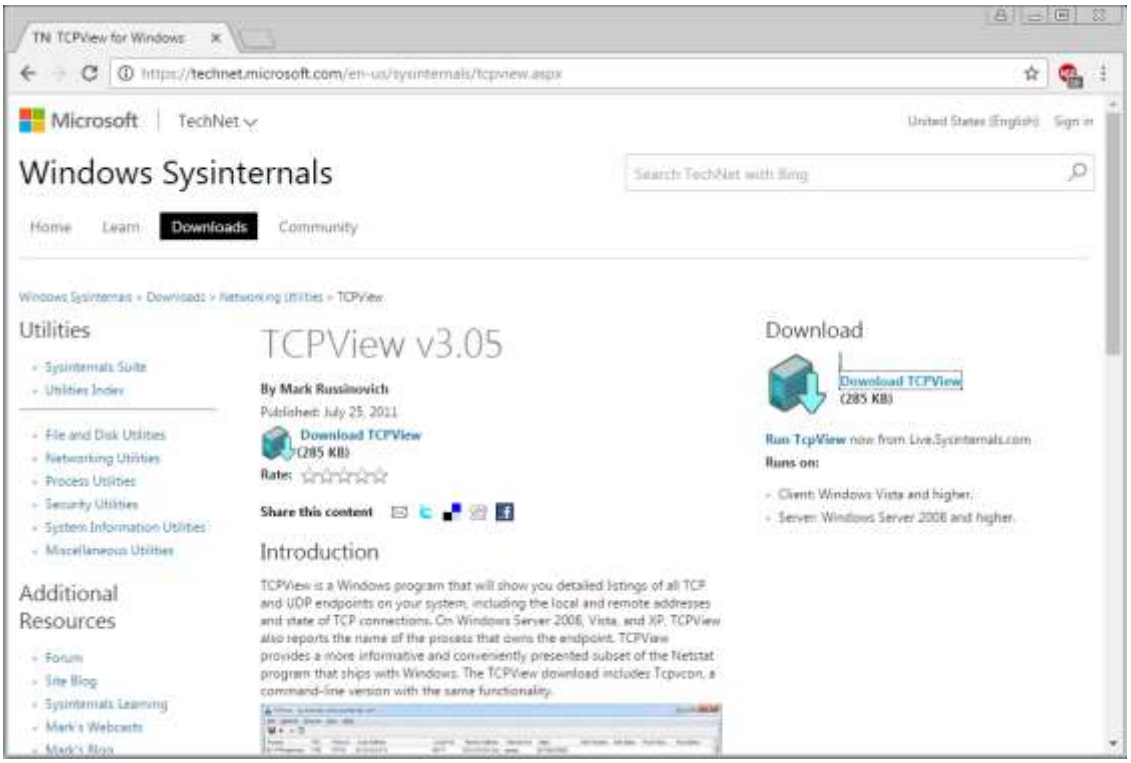
- Computadora con acceso a Internet
- Software TCPView

Instrucciones

Parte 1: Descargar e instalar el software TCPView

a. Haga clic en el siguiente link para poder descargar TCPView.

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

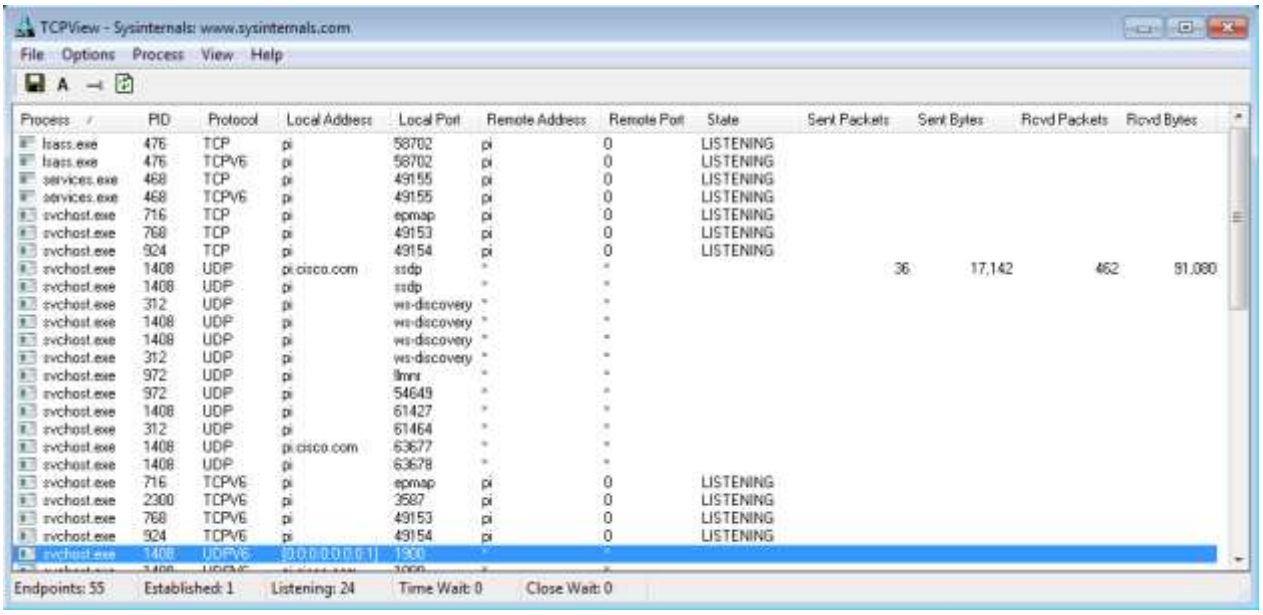


b. Crear una carpeta en el escritorio con el nombre de **"TCPView"**

c. Extraer el contenido del zip en esta carpeta nueva.

d. Inicia la aplicación Tcpview.

e. Finalmente, aceptar los términos de la licencia de software.



Parte 2: Respondan las siguientes preguntas.

a. ¿Cuántos endpoints aparecen en la lista?

b. ¿Cuántos están escuchando?

c. ¿Cuántos endpoints están establecidos?

Parte 3: Utilizar un navegador para observar la ventana de TCPView.

a. Abrir el menú de opciones y hagan clic en “Always on Top” (“Siempre visible”).

Nota: Utilizar la sección de Ayuda del programa para poder responder las siguientes preguntas.

b. Abrir cualquier navegador.

¿Qué sucede en la ventana TCPView?

c. Ir a cisco.com.

¿Qué sucede en la ventana TCPView?

d. Cerrar el navegador.

¿Qué sucede en la ventana TCPView?

¿Qué pueden significar los colores?

Nota: Para cerrar un proceso directamente, haga clic derecho en el proceso y elija **Finalizar proceso**. Este método puede hacer que un programa o el sistema operativo se vuelvan inestables. Solo debemos finalizar procesos cuando sabemos que es seguro hacerlo. Este método puede utilizarse para impedir que el malware se comunique.