

## 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.

## Actividad de Clase - ¿Qué está sucediendo?

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

The screenshot shows a Microsoft TechNet page for Windows Sysinternals. The main content is about the TCPView utility version 3.05. It includes a download link for the executable (TCPView.exe) which is 285 KB in size. The page also provides information about the software's compatibility with Windows Vista and later versions.

**Utilities**

- Sysinternals Suite
- Utilities Index
- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

**Additional Resources**

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Blog

**TCPView v3.05**

By Mark Russinovich  
Published: July 25, 2011

[Download TCPView \(285 KB\)](#)

Rate:

Share this content: [Email](#) [Print](#) [Facebook](#) [Twitter](#) [LinkedIn](#)

**Introduction**

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes TcpView, a command-line version with the same functionality.

**Download**

[Download TCPView \(285 KB\)](#)

Run TCPView now from Live.Systernals.com

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

- Crear una carpeta en el escritorio con el nombre de "**TCPView**"
- Extraer el contenido del zip en esta carpeta nueva.
- Inicia la aplicación Tcpview.
- Finalmente, aceptar los términos de la licencia de software.

The screenshot shows the TCPView application window running on a Windows operating system. The main interface displays a table of network endpoints. The columns include Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Rcvd Packets, and Rcvd Bytes. The table lists numerous entries, primarily for svchost.exe processes, showing various ports and states like LISTENING or TIME\_WAIT.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
svchost.exe	476	TCP	0.0.0.0	58702	0.0.0.0	0	LISTENING				
svchost.exe	476	TCPv6	0.0.0.0	58702	0.0.0.0	0	LISTENING				
services.exe	468	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING				
services.exe	468	TCPv6	0.0.0.0	49155	0.0.0.0	0	LISTENING				
svchost.exe	716	TCP	0.0.0.0	epmap	0.0.0.0	0	LISTENING				
svchost.exe	768	TCP	0.0.0.0	49153	0.0.0.0	0	LISTENING				
svchost.exe	924	TCP	0.0.0.0	49154	0.0.0.0	0	LISTENING				
svchost.exe	1408	UDP	0.0.0.0	ssdp	0.0.0.0	*	*	36	17,142	462	51,080
svchost.exe	1408	UDP	0.0.0.0	ssdp	0.0.0.0	*	*				
svchost.exe	312	UDP	0.0.0.0	wi-discovery	0.0.0.0	*	*				
svchost.exe	1408	UDP	0.0.0.0	wi-discovery	0.0.0.0	*	*				
svchost.exe	1408	UDP	0.0.0.0	wi-discovery	0.0.0.0	*	*				
svchost.exe	312	UDP	0.0.0.0	llmnr	0.0.0.0	*	*				
svchost.exe	972	UDP	0.0.0.0	54649	0.0.0.0	*	*				
svchost.exe	1408	UDP	0.0.0.0	61427	0.0.0.0	*	*				
svchost.exe	312	UDP	0.0.0.0	61464	0.0.0.0	*	*				
svchost.exe	1408	UDP	0.0.0.0	63677	0.0.0.0	*	*				
svchost.exe	1408	UDP	0.0.0.0	63678	0.0.0.0	*	*				
svchost.exe	716	TCPv6	0.0.0.0	epmap	0.0.0.0	0	LISTENING				
svchost.exe	2300	TCPv6	0.0.0.0	3587	0.0.0.0	0	LISTENING				
svchost.exe	768	TCPv6	0.0.0.0	49153	0.0.0.0	0	LISTENING				
svchost.exe	924	TCPv6	0.0.0.0	49154	0.0.0.0	0	LISTENING				
svchost.exe	1408	UDPF6	0.0.0.0	1900	0.0.0.0	*	*				
svchost.exe	3408	UDPF6	0.0.0.0	3000	0.0.0.0	*	*				

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

## 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.