



## Atividade de Classe - O que está acontecendo?

### Objetivos

Identifique os processos em execução em um computador, o protocolo que eles estão usando e seus endereços de porta local e remota.

**Parte 1: Baixe e instale o software TCPView.**

**Parte 2: Responda às seguintes perguntas.**

**Parte 3: Use um navegador e observe a janela TCPView.**

### Histórico/Cenário

Para que um hacker estabeleça uma conexão com um computador remoto, uma porta deve estar escutando nesse dispositivo. Isso pode ser devido a infecção por malware ou a uma vulnerabilidade em um software legítimo. Um utilitário, como o TCPView, pode ser usado para detectar portas abertas, monitorá-las em tempo real e fechar portas e processos ativos que as utilizam.

### Recursos necessários

- PC com acesso à Internet
- Software TCPView

### Instruções

#### **Parte 1: Baixe e instale o software TCPView.**

- a. Clique no link abaixo para acessar a página de download do TCPView.

## Atividade de Classe - O que está acontecendo?

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

The screenshot shows the TechNet Microsoft website for Windows Sysinternals. The URL in the address bar is https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx. The page title is "TN TCPView for Windows". The main content is about "TCPView v3.05" by Mark Russinovich, published on July 25, 2011. It includes a download link for "Download TCPView (285 KB)" and a "Run TcpView now from Live.Sysinternals.com" button. The "Downloads" tab is selected in the navigation menu. On the left, there's a sidebar for "Utilities" and "Additional Resources". A screenshot of the TCPView application window is shown at the bottom right.

- b. Crie uma pasta na área de trabalho chamada **TCPView**.
- c. Extraia o conteúdo do zip para esta nova pasta.
- d. Inicie o aplicativo Tcpview.
- e. Finalmente, concorde com os termos de licença de software.

The screenshot shows the TCPView application window. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The main interface displays a table of network endpoints. The columns are: 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, mostly for svchost.exe processes, showing various ports like 58702, 49155, 49153, 49154, and 63678. The "State" column shows mostly LISTENING. The "Sent Packets" and "Rcvd Packets" columns have values like 36, 17,142, 462, and 91,080. At the bottom, there are status bars for "Endpoints: 55", "Established: 1", "Listening: 24", "Time Wait: 0", and "Close Wait: 0".

## **Atividade de Classe - O que está acontecendo?**

---

### **Parte 2: Responda às perguntas a seguir.**

- a. Quantos Endpoints estão listados?
  
- b. Quantos estão escutando?
  
- c. Quantos endpoints são estabelecidos?

### **Parte 3: Use um navegador e observe a janela TCPView.**

- a. Abra o menu Opções e clique em “Sempre no topo”.

**Observação:** Use a seção Ajuda do programa para ajudá-lo a responder às perguntas a seguir.

- b. Abra qualquer navegador.

O que acontece na janela do TCPView?

- c. Navegue até cisco.com.

O que acontece na janela do TCPView?

- d. Feche o navegador.

O que acontece na janela do TCPView?

O que você acha que as cores significam?

**Observação:** Para fechar um processo diretamente, clique com o botão direito do mouse no processo e escolha **Finalizar Processo**. Usar esse método pode fazer com que um programa ou o sistema operacional se torne instável. Apenas termine os processos que você sabe que são seguros para terminar. Este método pode ser usado para impedir a comunicação de malware.