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

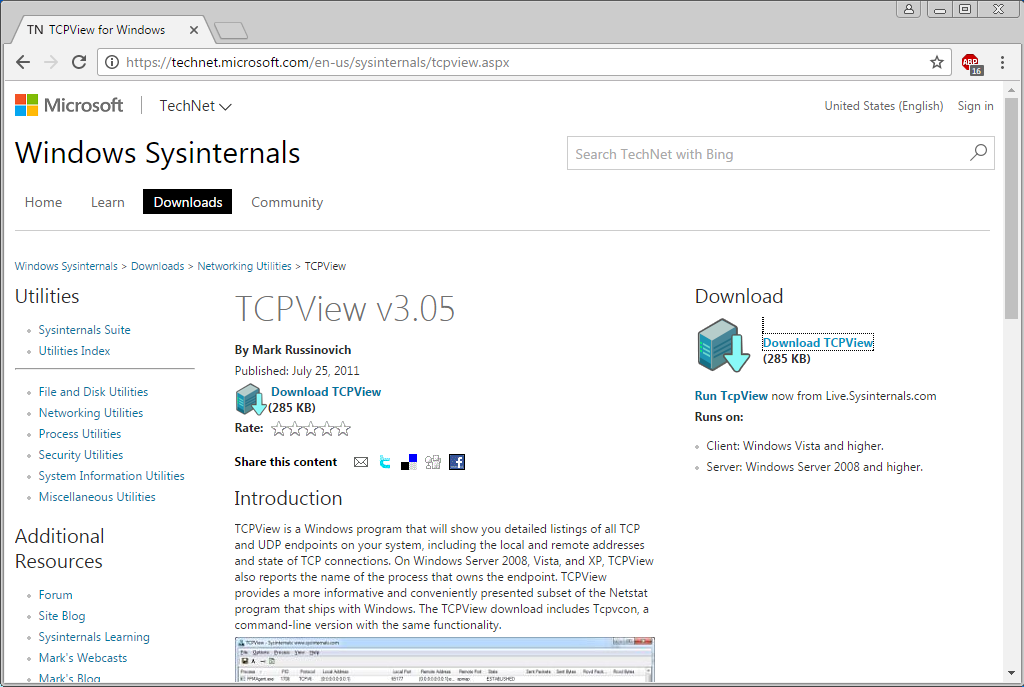
* PC com acesso à Internet
* Software TCPView

# Instruções

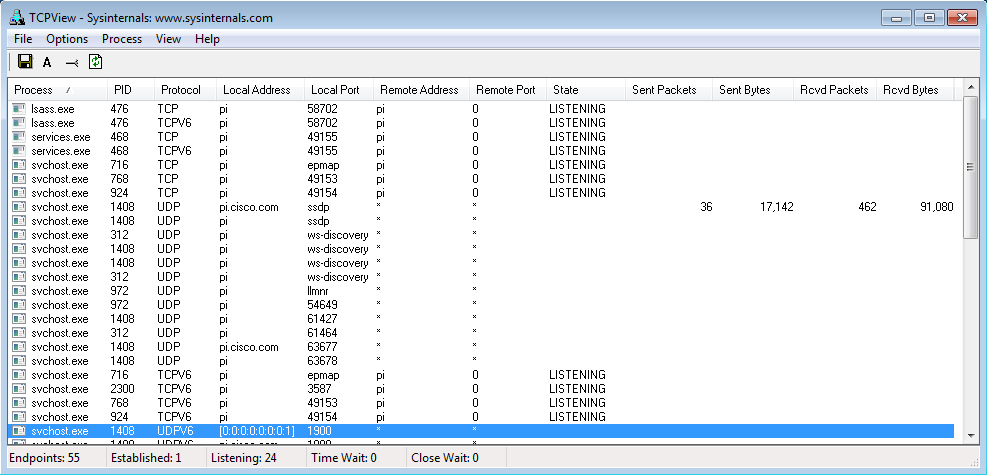
## Baixe e instale o software TCPView.

* + 1. Clique no link abaixo para acessar a página de download do TCPView.

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



* + 1. Crie uma pasta na área de trabalho chamada **TCPView**.
    2. Extraia o conteúdo do zip para esta nova pasta.
    3. Inicie o aplicativo Tcpview.
    4. Finalmente, concorde com os termos de licença de software.



## Responda às perguntas a seguir.

### Perguntas:

* + 1. Quantos Endpoints estão listados?

Digite suas respostas aqui.

* + 1. Quantos estão escutando?

Digite suas respostas aqui.

* + 1. Quantos endpoints são estabelecidos?

Digite suas respostas aqui.

## Use um navegador e observe a janela TCPView.

* + 1. 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.

* + 1. Abra qualquer navegador.

### Pergunta:

O que acontece na janela do TCPView?

Digite suas respostas aqui.

* + 1. Navegue até cisco.com.

### Pergunta:

O que acontece na janela do TCPView?

Digite suas respostas aqui.

* + 1. Feche o navegador.

### Perguntas:

O que acontece na janela do TCPView?

Digite suas respostas aqui.

O que você acha que as cores significam?

Digite suas respostas aqui.

**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.

Fim do documento