Atividade da Classe - Identificar Processos em Execução

# Objetivos

Neste laboratório, você usará o TCP/UDP Endpoint Viewer, uma ferramenta no Sysinternals Suite, para identificar quaisquer processos em execução no seu computador.

Parte 1: Baixar o Windows Sysinternals Suite.

Parte 2: Inicie TCP/UDP Endpoint Viewer.

Parte 3: Explore os processos em execução.

Parte 4: Explore um processo iniciado pelo usuário.

# Histórico/Cenário

Neste laboratório, você explorará processos. Processos são programas ou aplicativos em execução. Você explorará os processos usando o Explorador de Processos no Windows Sysinternals Suite. Você também iniciará e observará um novo processo.

# Recursos necessários

* 1 PC Windows com acesso à internet

# Instruções

## Baixe o Windows Sysinternals Suite.

* + 1. Navegue até o link a seguir para baixar o Windows Sysinternals Suite:

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

* + 1. Após a conclusão do download, clique com o botão direito do mouse no arquivo zip e escolha **Extrair tudo...**, para extrair os arquivos da pasta. Escolha o nome e o destino padrão na pasta Downloads e clique em **Extrair**.
    2. Saia do navegador da Web.

## Inicie TCP/UDP Endpoint Viewer.

* + 1. Navegue até a pasta SysInternalsSuite com todos os arquivos extraídos.
    2. Abra **Tcpview.exe**. Aceite o Contrato de Licença do Process Explorer quando solicitado. Clique em **Sim** para permitir que este aplicativo faça alterações em seu dispositivo.
    3. Saia do Explorer e feche todas as aplicações atualmente em execução.

## Explore os processos em execução.

* + 1. O TCPView lista o processo que está atualmente no seu PC Windows. Neste momento, apenas os processos do Windows estão em execução.
    2. Dê um clique duplo **lsass.exe**.

### Pergunta:

O que é lsass.exe? Em que pasta ele está localizado?

Digite suas respostas aqui.

* + 1. Feche a janela de propriedades para lsass.exe quando terminar.
    2. Exiba as propriedades dos outros processos em execução.

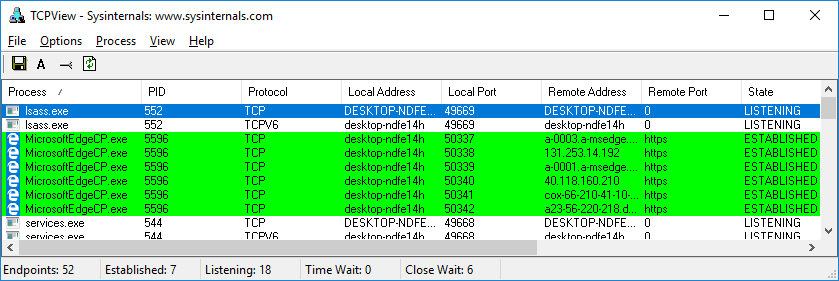
**Observação**: Nem todos os processos podem ser consultados para obter informações sobre propriedades.

## Explore um processo iniciado pelo usuário.

* + 1. Abra um navegador da Web, como o Microsoft Edge.

O que você observou na janela do TCPView?

Digite suas respostas aqui.

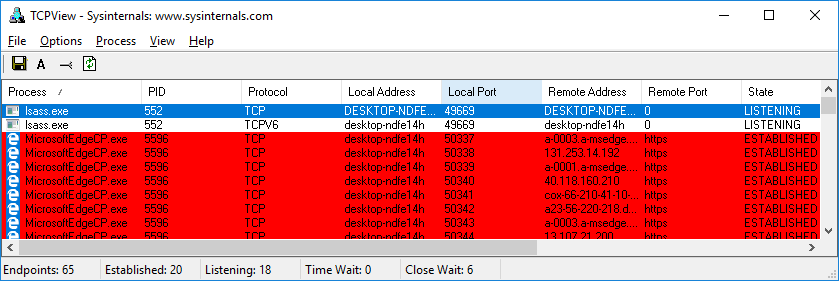


* + 1. Feche o navegador da Web.

### Pergunta:

O que você observou na janela do TCPView?

Digite suas respostas aqui.



* + 1. Reabra o navegador Web. Pesquise alguns dos processos listados no TCPView. Anote suas descobertas.

Digite suas respostas aqui.