

## 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

#### Parte 1: Baixe o Windows Sysinternals Suite.

- Navegue até o link a seguir para baixar o Windows Sysinternals Suite:  
<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- 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**.
- Saia do navegador da Web.

#### Parte 2: Inicie TCP/UDP Endpoint Viewer.

- Navegue até a pasta SysInternalsSuite com todos os arquivos extraídos.
- 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.
- Saia do Explorer e feche todas as aplicações atualmente em execução.

#### Parte 3: Explore os processos em execução.

- O TCPView lista o processo que está atualmente no seu PC Windows. Neste momento, apenas os processos do Windows estão em execução.
- Dê um clique duplo **lsass.exe**.  
O que é lsass.exe? Em que pasta ele está localizado?

## Atividade da Classe - Identificar Processos em Execução

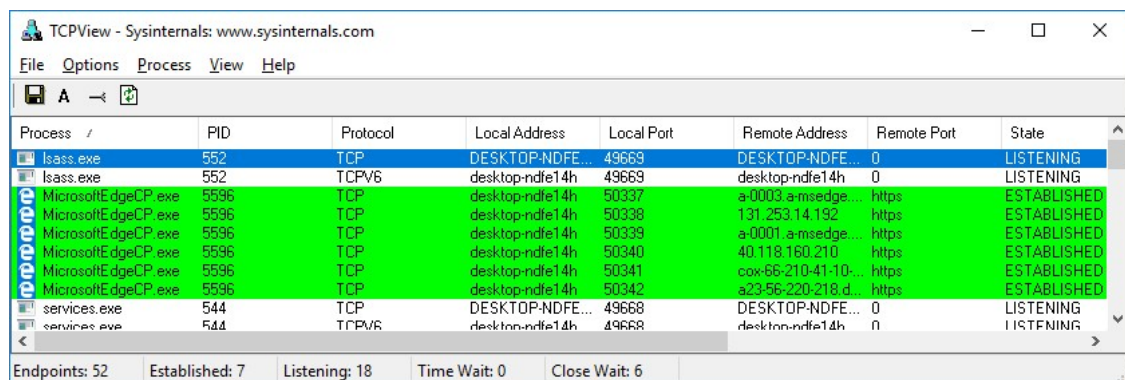
- c. Feche a janela de propriedades para lsass.exe quando terminar.
- d. Exiba as propriedades dos outros processos em execução.

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

### Parte 4: Explore um processo iniciado pelo usuário.

- a. Abra um navegador da Web, como o Microsoft Edge.

O que você observou na janela do TCPView?



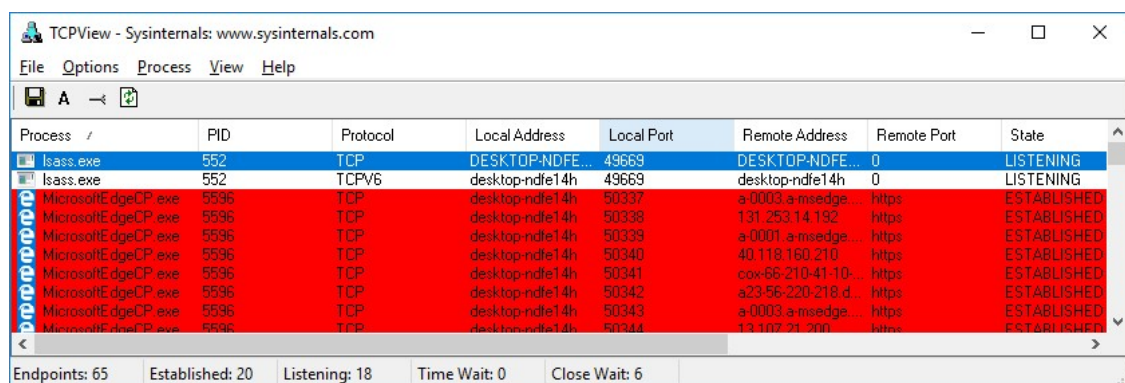
The screenshot shows the TCPView application window. The process list on the left includes lsass.exe (PID 552) and several instances of Microsoft Edge (PID 5596). The main table displays network connections. lsass.exe is listening on port 49669. Microsoft Edge has several established connections to various remote addresses on port 49669. The status bar at the bottom shows 52 endpoints, 7 established, 18 listening, 0 time wait, and 6 close wait.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
lsass.exe	552	TCPV6	desktop-ndfe14h	49669	desktop-ndfe14h	0	LISTENING
Microsoft Edge	5596	TCP	desktop-ndfe14h	50337	a-0003.a-msedge...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50338	131.253.14.192	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50339	a-0001.a-msedge...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50340	40.118.160.210	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50341	cow-66-210-41-10...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50342	a23-56-220-218.d	https	ESTABLISHED
services.exe	544	TCP	DESKTOP-NDFE...	49668	DESKTOP-NDFE...	0	LISTENING
services.exe	544	TCPV6	desktop-ndfe14h	49668	desktop-ndfe14h	0	LISTENING

Endpoints: 52 | Established: 7 | Listening: 18 | Time Wait: 0 | Close Wait: 6

- b. Feche o navegador da Web.

O que você observou na janela do TCPView?



The screenshot shows the TCPView application window after closing Microsoft Edge. The process list on the left still includes lsass.exe (PID 552) and Microsoft Edge (PID 5596). The main table shows that the established connections for Microsoft Edge have been terminated. The status bar at the bottom shows 65 endpoints, 20 established, 18 listening, 0 time wait, and 6 close wait.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	552	TCP	DESKTOP-NDFE...	49669	DESKTOP-NDFE...	0	LISTENING
lsass.exe	552	TCPV6	desktop-ndfe14h	49669	desktop-ndfe14h	0	LISTENING
Microsoft Edge	5596	TCP	desktop-ndfe14h	50337	a-0003.a-msedge...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50338	131.253.14.192	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50339	a-0001.a-msedge...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50340	40.118.160.210	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50341	cow-66-210-41-10...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50342	a23-56-220-218.d	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50343	a-0003.a-msedge...	https	ESTABLISHED
Microsoft Edge	5596	TCP	desktop-ndfe14h	50344	131.253.14.192	https	ESTABLISHED

Endpoints: 65 | Established: 20 | Listening: 18 | Time Wait: 0 | Close Wait: 6

- c. Reabra o navegador Web. Pesquise alguns dos processos listados no TCPView. Anote suas descobertas.

