Laboratório - Explorando Processos, Threads, Handles e Registro do Windows

Objetivos

Neste laboratório, você explorará os processos, threads e manipuladores usando o Process Explorer no SysInternals Suite. Você também usará o Registro do Windows para alterar uma configuração.

Parte 1: Explorando Processos

Parte 2: Explorando Threads e Alças

Parte 3: Explorando o Registro do Windows

Recursos necessários

- 1 PC Windows com acesso à internet

Instruções

Parte 1: Explorando Processos

Nesta parte, você explorará processos. Processos são programas ou aplicativos em execução. Você explorará os processos usando o Process Explorer no Windows SysInternals Suite. Você também iniciará e observará um novo processo.

Etapa 1: Baixe o Windows SysInternals Suite.

a. Navegue até o link a seguir para baixar o Windows SysInternals Suite:

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

b. Após a conclusão do download, extraia os arquivos da pasta.

c. Deixe o navegador da Web aberto para as etapas a seguir.

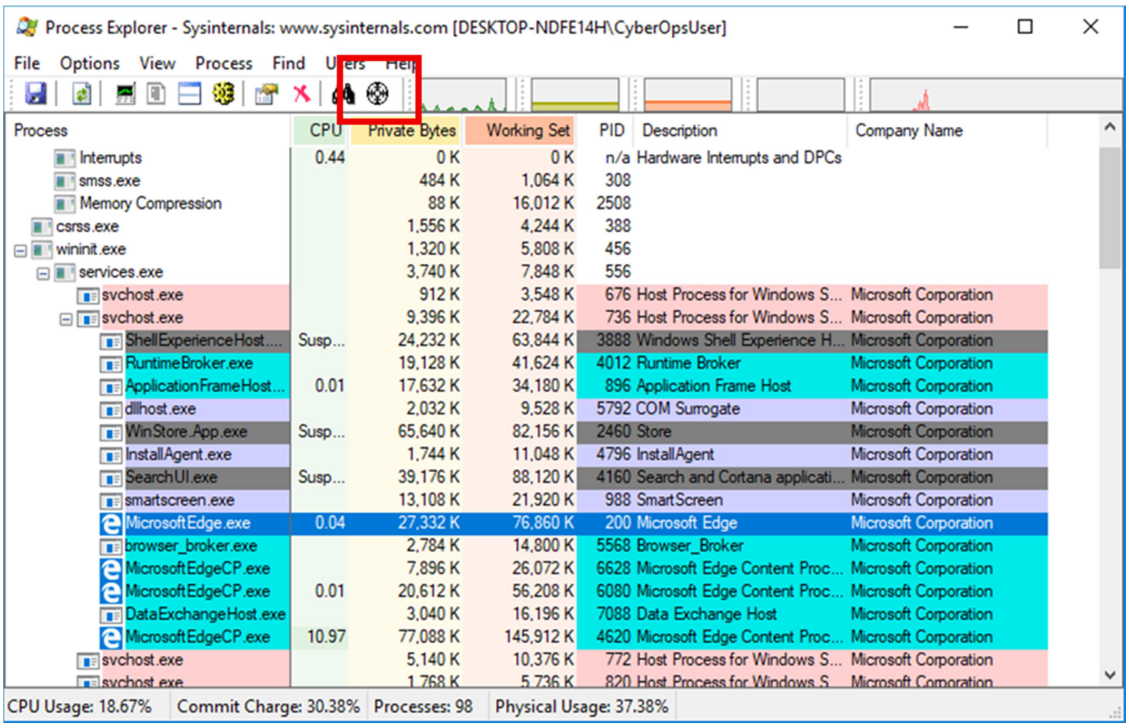
Etapa 2: Explore um processo ativo.

a. Navegue até a pasta SysInternalsSuite com todos os arquivos extraídos.

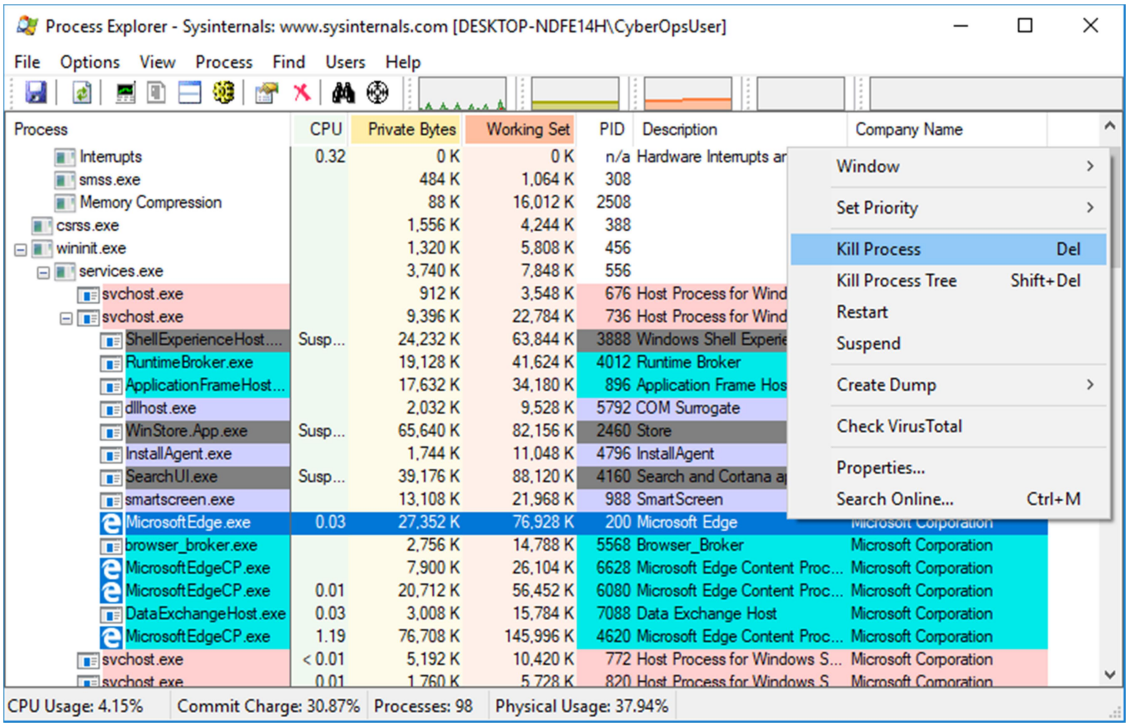
b. Abra **procexp.exe**. Aceite o Contrato de Licença do Process Explorer quando solicitado.

c. O Process Explorer exibe uma lista de processos ativos no momento.

d. Para localizaro processo do navegador da Web, arraste o ícone **Processo da Janela Localizar** para a janela aberta do navegador da Web. O Microsoft Edge foi usado neste exemplo.



e. O processo do Microsoft Edge pode ser encerrado no Process Explorer. Clique com o botão direito no processo selecionado e selecione **Eliminar Processo** Clique em **OK** para continuar.



O que aconteceu com a janela do navegador da Web quando o processo é eliminado?

Etapa 3: Inicie outro processo.

a. Abra um prompt de comando. (**Iniciar** > pesquisar **Prompt de Comando** > selecione **Prompt de Comando**)

b. Arraste o ícone **Processo da Janela Localizar** para a janela Prompt de Comando e localize o processo de Prompt de Comando realçado no Process Explorer.

c. O processo para o prompt de comando é cmd.exe. Seu processo pai é o processo explorer.exe. O cmd.exe tem um processo filho, conhost.exe.

d. Navigate to the Command Prompt window. Inicie um ping no prompt e observe as alterações no processo cmd.exe.

   O que aconteceu durante o processo de ping?

e. Ao revisar a lista de processos ativos, você acha que o processo filho conhost.exe pode ser suspeito. Para procurar conteúdo malicioso, clique com o botão direito do mouse em **conhost.exe** e selecione **Verificar VirusTotal**. Quando solicitado, clique em **Sim** para concordar com os Termos de Serviço VirusTotal. Em seguida, clique em **OK** para o próximo prompt.

f. Expanda a janela do Process Explorer ou role para a direita até ver a coluna VirusTotal. Clique no link sob a coluna VirusTotal. O navegador da Web padrão é aberto com os resultados em relação ao conteúdo malicioso do conhost.exe.

g. Clique com o botão direito no processo cmd.exe e selecione **Eliminar Processo**

   O que aconteceu com o processo filho conhost.exe?

Parte 2: Explorando Threads e Alças

Nesta parte, você vai explorar tópicos e alças. Os processos têm um ou mais threads. Um thread é uma unidade de execução em um processo. Um identificador é uma referência abstrata a blocos de memória ou objetos gerenciados por um sistema operacional. Você usará o Process Explorer (procexp.exe) no Windows SysInternals Suite para explorar os threads e identificadores.

Etapa 1: Explore tópicos.

a. Abra um prompt de comando.

b. Na janela Process Explorer, clique com o botão direito do mouse em conhost.exe e Selecionar **Propriedades...** Clique na guia **Threads** para exibir os threads ativos para o processo conhost.exe. Clique em **OK** para continuar se solicitado por uma caixa de diálogo de aviso.

c. Examine os detalhes do thread.

Que tipo de informação está disponível na janela Propriedades?

d. Clique em **OK** para continuar.

Etapa 2: Explore alças.

a. No Process Explorer, clique em **Exibir** > selecione Modo de **Exibição de Painel Inferior** > **Alças** para exibir os identificadores associados ao processo conhost.exe.

Examine as alças. Para que apontam as alças?

b. Feche o Process Explorer quando terminar.

Parte 3: Explorar o Registro do Windows

O Registro do Windows é um banco de dados hierárquico que armazena a maioria dos sistemas operacionais e configurações de ambiente de trabalho.

a. Para acessar o Registro do Windows, clique em **Iniciar** > Pesquisar **regedit** e selecione **Editor do Registro**. Clique em **Sim** quando solicitado a permitir que este aplicativo faça alterações.

O Editor do Registro tem cinco hives. Estas hives estão no nível superior do registo.

- HKEY_CLASSES_ROOT é na verdade a subchave Classes de HKEY_LOCAL_MACHINE\ Software\ Ele armazena informações usadas por aplicativos registrados como associação de extensão de arquivo, bem como um identificador programático (ProgID), ID de classe (CLSID) e dados de ID de interface (IID).
- HKEY_CURRENT_USER contém as configurações e configurações para os usuários que estão conectados no momento.
- HKEY_LOCAL_MACHINE armazena informações de configuração específicas do computador local.
- HKEY_USERS contém as configurações e configurações para todos os usuários no computador local. HKEY_CURRENT_USER é uma subchave de HKEY_USERS.
- HKEY_CURRENT_CONFIG armazena as informações de hardware usadas na inicialização pelo computador local.

b. Em uma etapa anterior, você aceitou o EULA para Process Explorer. Navegue até a chave de registro EulaAccepted para Process Explorer.

Clique para selecionar Process Explorer em **HKEY_CURRENT_USER** > **Software** > **Sysinternals** > **Process Explorer**. Role para baixo para localizar a chave **EulaAccepted**. Atualmente, o valor para a chave de registro EulaAccepted é 0x00000001 (1).

c. Clique duas vezes na chave de registro **EULAAceite**. Atualmente, os dados do valor são definidos como 1. O valor de 1 indica que o EULA foi aceito pelo usuário.

d. Altere o **1** para **0** para dados de valor. O valor 0 indica que o EULA não foi aceito. Clique em **OK** para continuar.

Qual é o valor para esta chave de registo na coluna Dados?

e. Abra o **Process Explorer**. Navegue até a pasta onde você baixou o SysInternals. Abra a pasta **SysInternalsSuite** > Abrir **procexp.exe**.

   Quando você abre o Process Explorer, o que você viu?