Windows实验 - 识别正在运行的进程

1. 目标

在本实验中，同学们将使用 TCP/UDP 终端查看器（Sysinternals Suite 中的工具）识别计算机上任何正在运行的进程。

1. 背景/场景

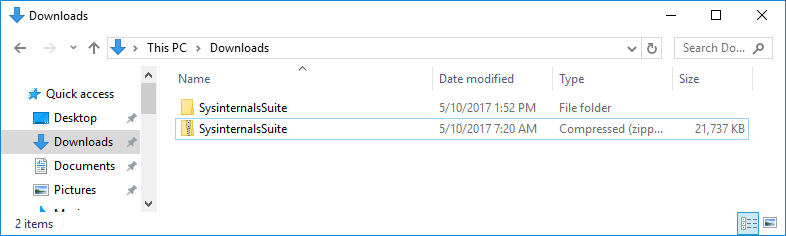
在本实验中，同学们将了解进程的相关知识。进程是指正在执行的程序或应用。同学们将使用 Windows Sysinternals Suite 中的进程资源管理器了解进程。同学们还将启动和观察新进程。

1. 所需资源

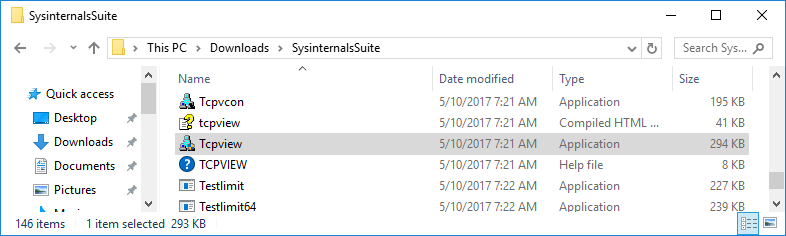
* 1 台接入互联网的 Windows PC
  1. 下载 Windows Sysinternals Suite。
     1. 导航到下面的链接，下载 Windows Sysinternals Suite：

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

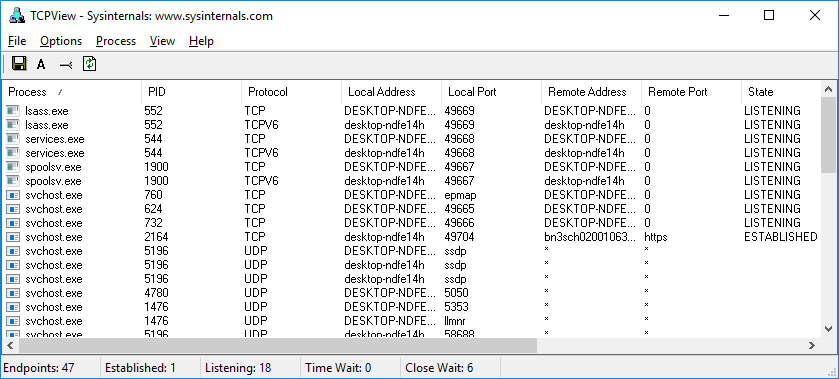
* + 1. 下载完成后，右键点击 zip 文件，选择**全部解压…**，解压文件夹中的文件。选择“下载”文件夹中的默认名称和目标位置，然后点击**解压**。
    2. 退出 Web 浏览器。
  1. 启动 TCP/UDP 终端查看器。
     1. 导航到包含所有解压文件的 SysinternalsSuite 文件夹。



* + 1. 打开 **Tcpview.exe**。系统提示时，接受《进程资源管理器许可协议》。点击**是**，允许此应用对同学们的设备进行更改。



* + 1. 退出文件资源管理器，然后关闭所有当前正在运行的应用。
  1. 了解正在运行的进程。
     1. TCPView 会列出 Windows PC 上当前正在运行的进程。当前只有 Windows 进程正在运行。



* + 1. 双击 **lsass.exe**。

Lsass.exe 是什么？它在哪个文件夹中？

答：用于本地安全和登陆策略，本地安全C:\Windows\System32\lsass.exe。

完成时，关闭 lsass.exe 的属性窗口。

* + 1. 查看其他正在运行的进程的属性。

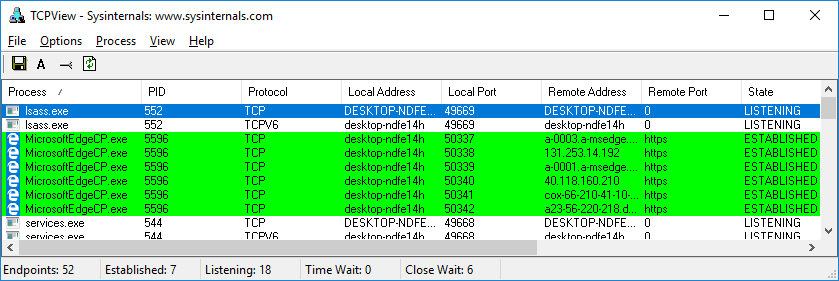
**注**：不是所有进程都可以查询属性信息。

* 1. 了解用户启动的进程。
     1. 打开 Web 浏览器，例如 Microsoft Edge。

同学们在 TCPView 窗口中看到了什么？

答：多出几个Microsoft进程。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

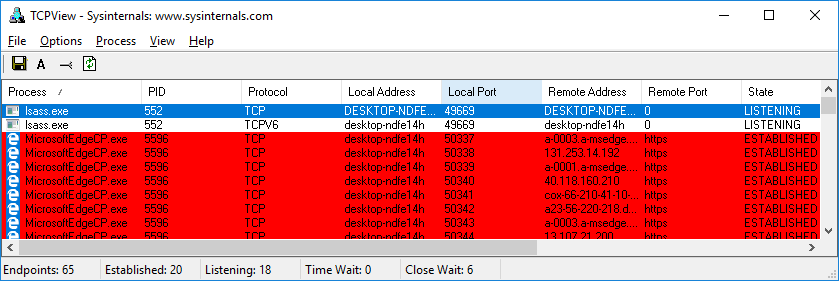


* + 1. 关闭 Web 浏览器。

同学们在 TCPView 窗口中看到了什么？

答： Microsoft进程变红并消失。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + 1. 重新打开 Web 浏览器。研究 TCPView 中列出的一些进程。记录同学们的发现。

MasterHelper.exe 7808 UDP DESKTOP-FF3RQSB 9997 \* \*

MicrosoftEdgeCP.exe 15080 TCP desktop-ff3rqsb 53834 a23-211-149-25.deploy.static.akamaitechnologies.com https ESTABLISHED 3 1,200 7 6,450

MicrosoftEdgeCP.exe 15080 TCP desktop-ff3rqsb 53834 a23-211-149-25.deploy.static.akamaitechnologies.com https ESTABLISHED 3 1,200 7 6,450

PID较之前发生改变。