Activity 03.1: Discover processes on Windows and Ubuntu

Purpose:
During this activity you will see what processes are running on Windows and Ubuntu

Objective:
Find out what processes run on Ubuntu and Windows.

NOTE: Prior to beginning this lab you should have downloaded the CyberPatriot Ubuntu virtual image.

Materials Required:
This exercise will require the following:
- The lastest VMware Player (http://www.vmware.com/products/player/)
- CyberPatriot Ubuntu Image
- Process Explorer (http://technet.microsoft.com/en-us/sysinternals/bb896653)

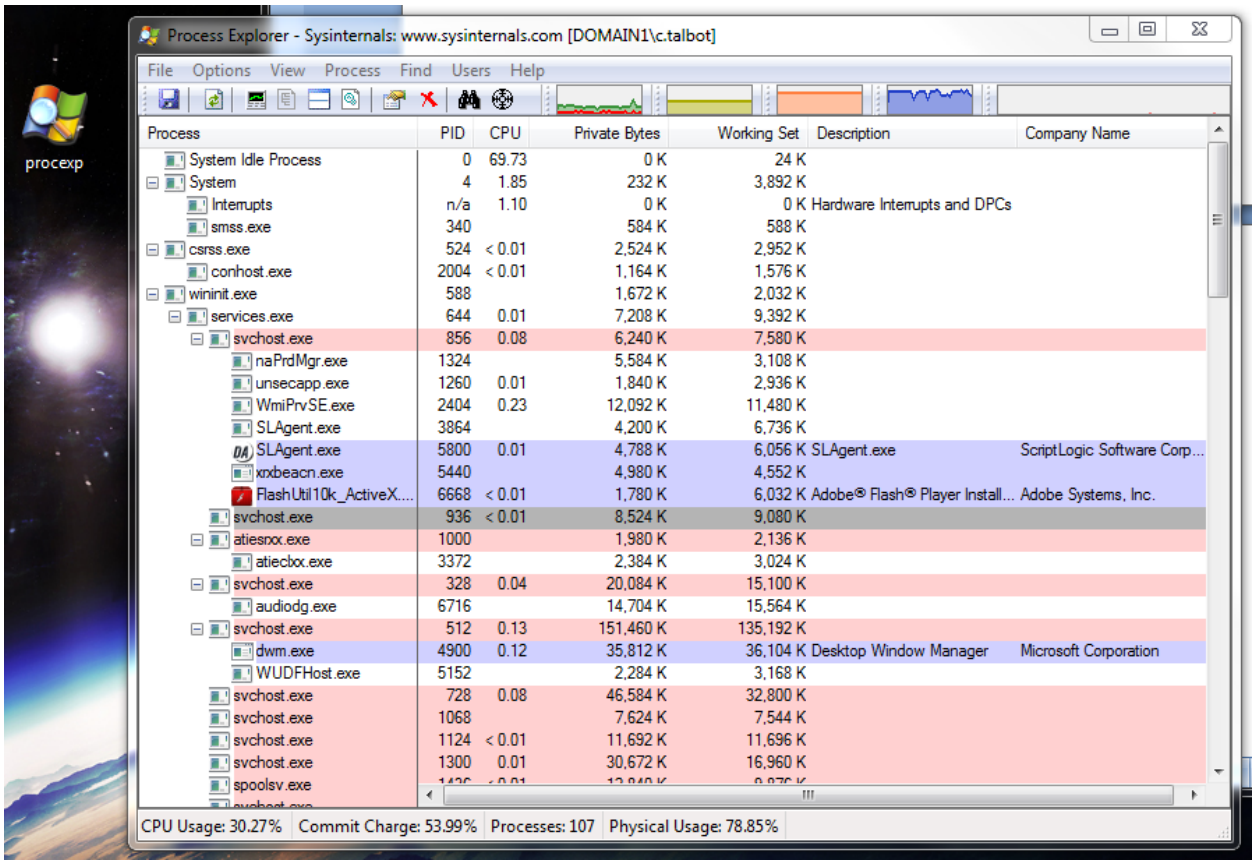
Estimated completion time: 20 - 30 minutes

Additional Information:
- None

Windows

Step 1: Download and Run Process Explorer

- http://technet.microsoft.com/en-us/sysinternals/bb896653
- Extract the zip file and run procexp.exe (if you can, run the program as an Administrator)
- Procecp.chm is a help file to help you understand how to use Process Explorer
    - Under View -> Select Columns… , You can select what columns you would like to see with Process Explorer
    - (If you are an Admin) Look at the “Process Network” and you can see if the processes are communicating over the Internet.
    - If you right click a column and select Properties, you can select “TCP/IP” and see what ports the process is listening on.



- In this, you will see many different processes running. A few to take a look at:
    - Svchost.exe
        - Why are there so many of this?
        - How many should be running on your computer?
    - Services.exe
    - Winlogon.exe
- Are there any processes you are not sure of what they are?
    - Look them up on an Internet search and see if you can find out what they do.

Ubuntu

Step 1: Load up a Bash Shell in Ubuntu and type:

- #ps aux
    - ps displays processes
    - aux displays all running processes
- #ps –A
    - –A displays all processes
- #ps –u CyberPatriot
    - Displays all processes run by CyberPatriot
- #top
    - The top command gives you a live view of the processes on your system
- #netstat
    - This shows a list of all open connections

Note that all of these commands have different arguments that display other information. CyberPatriot recommends looking at the man pages of each command to find out how to best use them.