Operating Systems

Lab: Process Management

Weight: 5% Marks: /76

Student Name:

Student ID:

Date:

This page was intentionally left blank.

Table of Contents

[Introduction 1](#_Toc168302504)

[Equipment and Materials 1](#_Toc168302505)

[Procedure 1](#_Toc168302506)

[Part A: Windows Processes 2](#_Toc168302507)

[Part B: Windows Process Information 3](#_Toc168302508)

[Part C: Thread Scheduling 6](#_Toc168302509)

[Part D: Process Explorer 8](#_Toc168302510)

[Part E: Linux Process Information 10](#_Toc168302511)

[Part F: Linux Process Management 13](#_Toc168302512)

[References 15](#_Toc168302513)

[Resources 15](#_Toc168302514)

Lab: Process Management

# Introduction

A process is a program in execution (e.g., it is running, waiting to run, waiting for input). Much of the usability and power of modern systems stems from the fact that there may be many processes in execution at any one time. Of course, this also leads to operating system complexity. Processes need to share resources like the CPU and the memory of a system, and they need to communicate with each other. They also need to be synchronized, controlled and scheduled.

Although default system behaviours are good enough for most users, high-performance environments such as web servers and database systems must be optimally configured. It’s important to understand and control process behaviour to obtain the most efficient use of resources.

In this lab, you’ll study several valuable tools that are available to monitor and control Windows and Linux processes.

**Important:** You are responsible for installing all **Windows** updates on the VM you create on your computer throughout the semester. Failure to do so will cause performance degradation. Ignore the updates at your own risk!

The Ubuntu VM doesn’t require constant updates unless you’re having issues with a package or tool.

## Equipment and Materials

* Windows and Linux VMs you installed in the previous lab.

# Procedure

1. Working in your lab groups, complete the activities and questions in each part of this lab. Ensure that each group member performs the steps on their own computer.
2. Submit one copy of the answers to your group’s shared submission folder on Brightspace before the posted due date.

## Part A: Windows Processes

1. Working in your lab groups, open the Windows VM on your respective computers and perform the following steps.
   1. Open Notepad.
   2. Start the Task Manager and select the **Processes** tab.
   3. Verify that the Notepad app is displayed in the list.
   4. Select the **Details** tab and sort the processes by Image Name.
   5. What is the Process ID and User of the Notepad process? (1 mark)

|  |
| --- |
| Answer:  Process ID (PID): 4568  KhrisellPorte |

**Note:** Type directly into the space provided and use the highlight function or change the font color of your answers. If the answer is different for each computer in the group, write down each group member’s name and their computer’s information.

1. Many other processes are displayed, and most of these are services. Research and briefly describe Windows services. (1 mark)

|  |
| --- |
| Answer: Windows services are specialized programs that operate in the background and provide various system-level functions without direct user interaction. They can be automatically initiated during the booting process of the operating system or manually started and stopped by the user or other applications. Windows services play a crucial role in managing tasks such as networking, security, printing, and system updates. The key characteristics of Windows services include operating in the background without a user interface, the ability to start automatically or be controlled manually through tools like the Services management console, Task Manager, or command-line tools, performing essential system-level tasks like managing network connections, handling updates, and managing printing, and running with specific user privileges to enhance security and system stability. By running continuously or on-demand, Windows services ensure the smooth operation and maintenance of the system. |

1. For each of the following processes, identify the user of each process, and then research and briefly describe their function.
   1. System Idle (2 marks)

|  |
| --- |
| Answer: The System Idle Process in Windows functions under the SYSTEM user account. Its main purpose is to occupy the CPU when the system is not performing any other active tasks. It operates with the lowest priority and serves as an indication of the system's idle state, displaying the amount of unused CPU capacity due to active processes. A high level of System Idle Process activity indicates that the CPU is not heavily utilized by other processes, indicating a significant amount of idle time for the system. |

* 1. Winlogon (2 marks)

|  |
| --- |
| Answer:  The Winlogon process is a critical component of the Windows operating system that handles user logins and logouts. It operates under the SYSTEM user account and performs various important functions, including:  1. User Authentication: Winlogon manages the process of authenticating user credentials by requesting and verifying the username and password entered at the login screen.  2. Loading User Profile: After successful authentication, Winlogon loads the user's profile, which includes their personalized settings and configurations.  3. Secure Attention Sequence (SAS): Winlogon responds to the Secure Attention Sequence (Ctrl+Alt+Delete) to ensure that this key combination brings up the security options screen. This screen provides options to lock the computer, change the password, or open Task Manager.  4. Session Management: It initializes the user session and handles session-specific details, such as launching the user's desktop environment and associated applications.  5. System Security: Winlogon plays a crucial role in maintaining system security. It locks the workstation when the user initiates a lock command or when the system screensaver with password protection is activated.  As a conclusion, the Winlogon process, operating under the SYSTEM user account, is vital for managing user logins, session initialization, and system security on Windows operating systems. |

* 1. Explorer (2 marks)

|  |
| --- |
| Answer:  The Explorer process, also referred to as Windows Explorer or explorer.exe, is a crucial element of the Windows operating system that is responsible for presenting the graphical user interface (GUI) for user interaction. It operates within the user's account that is presently logged in. The primary functions of the Explorer process encompass:  1. File Management:  - Explorer oversees the navigation, manipulation, and organization of files and folders. It furnishes the user interface for accessing, copying, moving, deleting, and renaming files.  2. Desktop Environment:  - It governs the desktop environment, encompassing the display of icons, taskbar, start menu, and system tray. The desktop and taskbar are fundamental components of the Explorer process.  3. Launching Applications:  - Explorer streamlines the process of launching applications. Users can initiate programs from the Start menu, taskbar, or desktop shortcuts, all managed by the Explorer process.  4. Search Functionality:  - The process offers search capabilities within Windows, enabling users to swiftly locate files, folders, and applications.  5. User Interface Customization:  - Explorer empowers users to personalize their desktop environment, including themes, wallpapers, and icon arrangements.  The Explorer process, operating under the account of the currently logged-in user, is indispensable for overseeing the Windows graphical user interface, file management operations, and overall user engagement with the operating system. |

## Part B: Windows Process Information

A process requires system resources for execution. Resource Monitor (perfmon.exe) is a Windows utility that displays real-time information about the use of hardware (CPU, memory, disk and network) and software (handles and modules).

1. If you haven’t already done so, open Notepad.
2. Open **Task Manager**, click the **Performance** tab and click the link on the bottom of the window to open **Resource Monitor**. How many active threads are there for the notepad process? (1 mark)

|  |
| --- |
| Answer:  Active Threads for Notepad Process: Approximately 4 threads |

1. Click the **Overview** tab and check the checkbox beside the **Notepad** image.
2. Type some text in Notepad and save the file on your desktop (use any name). How many threads are now used by Notepad? (1 mark)

|  |
| --- |
| Answer:  Threads after saving the file: Approximately 5 threads |

1. Select the **CPU** tab. Note that resources used by a process are accessed using a **handle**. List the types of handles used by Notepad (Hint: Find the dropdown list below the process list). (1 mark)

|  |
| --- |
| Answer:  File, Key, Event, Mutant, Section |

1. Sections of *system* code needed by a process may be stored in dynamic link libraries (.dll) of code, which are listed in the **Associated Modules** dropdown box. What is the PID of the modules used by the Notepad process? (1 mark)

|  |
| --- |
| Answer:  PID: 4568 |

1. Compare the PID of the modules to the PID of the notepad process itself. Why is the modules’ PID the same as the Notepad process? (Hint: Look at the memory usage of the notepad process). What’s the difference between shareable and private? (2 marks)

|  |
| --- |
| Answer: The PID of the modules matches that of the Notepad process due to the modules being loaded into the memory space of the Notepad process.  Shareable memory is accessible by multiple processes, whereas private memory is reserved solely for the Notepad process. |

1. Search for and run **Performance Monitor**.
2. Right-click the graph and select **Remove All Counters**.
3. Click the green **+** sign to add a counter.
4. Select the **Process > %Processor Time counter**, select the instance **notepad**, and then click the **Add>>** button and click **OK** to view the graph.
   1. Where is the value on the graph? (1 mark)

|  |
| --- |
| Answer: The value on the graph is shown in the vertical axis as a percentage of processor time used by the Notepad process. |

* 1. How can you make the value move? (1 mark)

|  |
| --- |
| Answer:  Actions performed in the Notepad application, such as typing text, opening files, or saving documents, can induce movement in the value displayed on the graph. This movement is a result of the Notepad process utilizing additional CPU resources, consequently altering the percentage of Processor Time exhibited on the graph. |

1. Each time a counter is selected in the *Add Counter* menu, view its description by checking the **Show Description** checkbox.
2. Add the following counters for the notepad instance. Briefly describe what each counter means.
   1. Elapsed Time (1 mark)

|  |
| --- |
| Answer:  The Elapsed Time counter quantifies the cumulative duration, in seconds, for which the Notepad process has been operational since its initiation. This counter serves as an indicator of the duration for which the process has remained active since its inception. |

* 1. Privileged Time (1 mark)

|  |
| --- |
| Answer:  The Privileged Time counter quantifies the proportion of CPU time utilized by the Notepad process for running code in kernel mode, encompassing system calls, device driver code, and other essential kernel-level tasks. |

* 1. User Time (1 mark)

|  |
| --- |
| Answer: The User Time counter quantifies the proportion of CPU time utilized by the Notepad process for executing tasks in user mode. This encompasses the duration dedicated to executing the application's proprietary code as well as any non-kernel mode operations, such as carrying out calculations, handling data, and executing user-defined functions. |

* 1. Handle Count (1 mark)

|  |
| --- |
| Answer: The Notepad process's Handle Count counter quantifies the overall quantity of handles that have been opened. Handles serve as references to various system resources, including files, registry keys, events, and other objects. This counter provides insight into the current utilization of these resources by the process. |

* 1. Priority Base (1 mark)

|  |
| --- |
| Answer: The base priority level of the Notepad process is assessed by the Priority Base counter. This priority is responsible for establishing the scheduling priority of the process within the operating system. A greater base priority indicates that the process is allocated a larger share of CPU time compared to other processes with lower priorities. |

* 1. Thread Count (1 mark)

|  |
| --- |
| Answer:  The Thread Count counter assesses the quantity of active threads in the Notepad process. Each thread signifies an individual path of execution, enabling the process to execute numerous tasks simultaneously. This counter reveals the current number of threads being utilized by the process. |

1. What is the difference between privileged and user mode? (1 mark)

|  |
| --- |
| Answer: Privileged Mode, also known as Kernel Mode, enables the operating system to carry out essential, low-level operations that involve direct interaction with hardware and system resources. In this mode, the operating system has unrestricted access to system memory and hardware, allowing it to effectively manage device drivers, system calls, and hardware interrupts.  The User Mode imposes restrictions on application software, preventing direct access to hardware and system memory. This mode ensures that applications operate within a controlled environment, promoting security and stability by preventing any direct interference with the core functions of the operating system. In User Mode, applications are required to make system calls to the operating system in order to request services that require higher privileges. |

1. Ensure that all the counters you added previously are active, and then perform some actions in Notepad. Take a screenshot of the graph in Performance Monitor (perfmon) and attach it here. (1 mark)

|  |
| --- |
| Answer: Attached to another file and will submit it along with this file, Sir. Thank you |

1. What is the purpose of having two separate modes of operation (i.e., privileged/kernel and user modes)? (1 mark)

|  |
| --- |
| Answer:  The existence of two distinct modes of operation, namely privileged (kernel) mode and user mode, serves the purpose of safeguarding system security and stability.  Kernel Mode: This mode grants the operating system the ability to carry out crucial tasks and establish direct communication with hardware and system resources without any limitations. By doing so, it ensures that vital system functions and hardware management are executed efficiently and securely.  User Mode: In contrast, user mode imposes restrictions on applications, preventing them from directly accessing hardware and critical system resources. This isolation serves as a protective measure, shielding the operating system and other applications from potential errors or malicious actions that may arise from user-level software. Consequently, this enhances the overall security and stability of the system. |

## Part C: Thread Scheduling

The Thread Scheduling utility can be useful when you’re debugging a multithreaded application and you’re unsure about the state of the threads running in the process.

1. Shut down the VM and change the number of processors to 1 CPU (for this part of the lab only).
2. Restart the VM.
3. Start a Notepad instance and open Performance Monitor.
4. Right-click the graph and select **Properties**.
5. Click the **Graph** tab, change the view to **Histogram bar** and change the vertical scale maximum to **7**. Click **OK**.
6. Click the **+** button on the toolbar to bring up the *Add Counters* dialog box.
7. Select the **Thread > Thread State** counter, and then check the **Show Description** checkbox to see the description of the thread state values.
8. Record down the thread state definition and the different state values. (2 marks)

|  |
| --- |
| Answer: In Windows, thread states represent the current status of a thread in its lifecycle. The different state values are:  Ready: The thread is ready to run but is not currently executing.  Running: The thread is currently executing on a CPU.  Standby: The thread is about to be scheduled for execution.  Terminated: The thread has finished execution and is no longer active.  Waiting: The thread is waiting for an event or a resource to become available.  Transition: The thread is ready for execution but waiting for a resource, such as memory paging.  Unknown: The state of the thread is not known. |

1. In the *Instances of selected object* dropdown box, select *<All instances>* and click on *Search*. The list of instances will be updated. Scroll down until you see the **notepad** process (notepad/0). Select it and click the **Add** button.
2. In the *Instances* list, scroll back to the **MMC** process (Microsoft Management Console process running the System Monitor) and select all the threads (mmc/0, mmc/1, and so on), and then add them to the chart by clicking the **Add** button.
3. Close the *Add Counters* box by clicking **OK**.
4. You should see the state of the Notepad thread. What is the state of Notepad? Why? (2 marks)

|  |
| --- |
| Answer: The Notepad process is currently in the "Running" state as it is actively engaged in executing tasks. When a process is involved in activities like processing user inputs, saving files, or performing any interactive tasks, it is considered to be in the Running state. This state signifies that the process is utilizing CPU time to execute its instructions and fulfill the user's requests. The Performance Monitor will display the graph reflecting the CPU usage and other resources utilized by the Notepad process. |

**Note:** Notice that one MMC thread is in the running state (number 2). This is the thread that's querying the thread states, so it's always displayed in the running state.

1. Can Notepad be in running state? (1 mark)

|  |
| --- |
| Answer: Yes, Notepad can be in an operational state. When Notepad is engaged in various activities such as acknowledging user input, handling data, or executing commands, it remains in an active state, effectively utilizing CPU resources to accomplish these tasks. |

1. How would you transition Notepad into running state? (1 mark)

|  |
| --- |
| Answer:  In order to activate Notepad and bring it into the operational state, various actions can be undertaken that necessitate the execution of tasks by the program. Several instances of such actions include typing text, opening a file, saving a file, and performing editing actions such as cut, copy, and paste. By engaging in these activities, Notepad will effectively utilize the CPU resources at its disposal and successfully transition into the running state. |

1. Can you see Notepad in the running state with your current setup? Why or why not? (2 marks)

|  |
| --- |
| Answer: Yes, the current setup displays Notepad in an active state.  If any actions are being carried out in Notepad, such as typing, opening, or saving files, the application will be running as it necessitates CPU resources to complete these tasks. This can be observed through the Performance Monitor, which will indicate the active status of the Notepad process and its CPU usage. The graphical representation and associated counters will confirm the running state of the process as a result of user interactions.  If there are no ongoing actions in Notepad, it may not remain in a continuous running state, as it will be idle and awaiting user input. |

1. If you’re not using a VM – What is the maximum number of processes you would be able to see in the running state at one time? Why? (2 marks)

|  |
| --- |
| Answer:  On a system with 8 logical processors, such as 4 physical cores with hyper-threading enabled, the maximum number of processes that can be seen in the running state simultaneously is 8. This is because each logical processor can handle one running thread at a time, and the operating system schedules processes across these logical processors. Therefore, any additional processes beyond the number of logical processors will be in a waiting state until a logical processor becomes available. |

1. Change the VM back to use multiple CPUs for better performance

## Part D: Process Explorer

All the system utilities discussed so far have their purposes and can be used when no external tools are present. Process Explorer (procexp) is a freeware task manager and system monitor for Microsoft Windows created by SysInternals, which has been acquired by Microsoft and re-branded as Windows Sysinternals. It provides the functionality of Windows Task Manager along with a rich set of features for collecting information about processes running on the user’s system (Wikipedia, 2023).

1. Download [Sysinternals Suite](https://learn.microsoft.com/en-us/sysinternals/downloads/) (https://learn.microsoft.com/en-us/sysinternals/downloads/).
2. Before you extract the tools from the zip file, remove the marker that tells Windows to treat the content of the file as coming from the internet and untrusted. This will remove the security warnings and content errors when you run any of the tools or view the help files.
   1. Right-click the **SysinternalsSuite.zip** file in folder you downloaded in the previous step and select **Properties**.
   2. Click the **General** tab, select the **Unblock** checkbox and click **OK**.
3. Extract the tools from the zipped file to a location you can easily remember, because you’ll use these tools in other labs in this course.
4. Open the **Sysinternals** folder and run **procexp.exe**.

The main window displays the process list arranged in a tree view showing parent/child process relationships. If you don’t have administrator privileges, you won’t see all the processes in the system. (The “user” in the VM is an admin.)

1. Use the Help (F1) to find out how to split the main window into an upper and lower pane.
   1. What is shown on the lower pane? What else can be shown there? (2 marks)

|  |
| --- |
| Answer: The lower pane in Process Explorer shows detailed information about the selected process. This can include Handles and DLLs. |

* 1. What do the mini graphs on the top show (from left to right)? (1 mark)

|  |
| --- |
| Answer: The mini graphs on the top of Process Explorer shows:  CPU usage  Memory usage  I/O activity  GPU usage |

1. One of the first things you’ll notice in the process list is its use of colour. Row colours distinguish different types or states of processes. Go to **Options > Configure Colors** to learn what each color represents.

**Note:** Even though you can customize the colours, it’s not recommended because many IT professionals rely on the default colours to differentiate the processes and to recognize suspicious activities.

1. Start a console window and launch Notepad from the command line by typing **notepad**.
2. View the new processes in Process Explorer.
3. Right-click the notepad process and open the **Properties** dialog box.

What is the parent process of notepad? Why? (2 marks)

|  |
| --- |
| Answer: The parent process of Notepad is the command prompt (cmd.exe) because Notepad was launched from the command line interface. |

1. Select the **Threads** tab and look for an error message regarding Dbghelp.dll.

This is one of Microsoft’s debug engines used for loading symbol files and resolving memory addresses to names. To fully trace and understand what the kernel is doing under the hood, you’ll need to configure the symbols.

* 1. Google **Microsoft debugging tools** or go to <https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk>.
  2. Download the standalone SDK.
  3. Install only the *Debugging Tools for Windows*.
  4. Open the Sysinternals’ *Process Explorer*, go to **Options > Configure Symbols** and point the Dbghelp.dll path to the debugging tools you just installed at:

C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\dbghelp.dll

Use the Microsoft public symbols at: srv\*c:\symbols\*https://msdl.microsoft.com/download/symbols

1. Reopen Notepad Properties and view the threads tab again.
   1. What does the context switches value represent? (1 mark)

|  |
| --- |
| Answer: The context switches value represents the number of times the operating system has switched the CPU from one thread to another. This is an important metric for understanding the multitasking efficiency of the system. |

* 1. What does the cycles values represent? (1 mark)

|  |
| --- |
| Answer: The cycles value represents the number of CPU cycles used by the thread. It measures the amount of processing time the thread has consumed on the CPU |

## Part E: Linux Process Information

1. View the file /proc/stat, and then briefly explain each of the following.
   1. cpu (1 mark)

|  |
| --- |
| Answer:  Shows combined CPU usage details, including time spent in different modes like user mode, system mode etc. |

* 1. ctxt (1 mark)

|  |
| --- |
| Answer:  Counts the number of context switches the system has done. |

* 1. processes (1 mark)

|  |
| --- |
| Answer:  Total number of processes created since the system started. |

* 1. procs\_running (1 mark)

|  |
| --- |
| Answer:  Number of processes currently able to run. |

* 1. procs\_blocked (1 mark)

|  |
| --- |
| Answer:  Number of processes currently waiting for I/O operations to finish. |

1. The ps command displays process’s status. Use the ps command without options, and then list and interpret the process’s attributes (use man for details about ps). (2 marks)

|  |
| --- |
| Answer:  PID: Process ID.  TTY: Terminal associated with the process.  TIME: Cumulative CPU time used by the process.  CMD: Command that started the process. |

1. Which ps command identifies only state, PID and command name of all processes? (Hint: Use the -o option.) (1 mark)

|  |
| --- |
| Answer:  The ‘ ps -o state,pid,comm’ command identifies the state, PID, and command name of all processes. |

1. Use man ps to identify the process state codes associated with the following process states.
   1. D – (1 mark)

|  |
| --- |
| Answer:  Uninterruptible sleep (usually I/O). |

* 1. R – (1 mark)

|  |
| --- |
| Answer:  Running or runnable (on run queue). |

* 1. T – (1 mark)

|  |
| --- |
| Answer:  Stopped by job control signal. |

* 1. X – (1 mark)

|  |
| --- |
| Answer:  Dead (should never be seen). |

* 1. Z – (1 mark)

|  |
| --- |
| Answer:  Defunct ("zombie") process |

1. What is the difference between a zombie process and an orphan process? (2 marks)

|  |
| --- |
| Answer:   1. Zombie Process: A process that has completed execution but still has an entry in the process table to report its status to its parent process. 2. Orphan Process: A process whose parent has terminated, leaving it without a parent process. The init process typically adopts orphan processes. |

1. The command top displays a summary of system information, and it dynamically shows the processes that currently have the highest priorities. Run top and record the following information.
   1. Total number of processes (tasks): (1 mark)

|  |
| --- |
| Answer:  Total processes in the system. |

* 1. Number of running processes: (1 mark)

|  |
| --- |
| Answer:  Processes currently running. |

* 1. Number of sleeping processes: (1 mark)

|  |
| --- |
| Answer:  Number of processes currently in the sleeping state. |

* 1. PID of the process top: (1 mark)

|  |
| --- |
| Answer:  The process ID of the top command itself. |

1. Press the letter **q** to quit top.
2. Many processes were displayed, and many of those are daemons. Research and briefly describe Linux daemons. (1 mark)

|  |
| --- |
| Answer: Linux daemons are background processes that typically start at boot time and provide various system services, such as logging, scheduling, and network management. They run without direct user interaction and often wait for specific events or requests to perform their tasks. |

1. Another name for a Linux thread is a lightweight process (LWP). In most systems, there is no difference between a thread and a LWP.
2. Use ps –eL to display status of all process threads. Find one command that started more than one thread (one PID repeated with different TIDs), and record the command, its PID and the TID of two of the threads: (1 mark)

|  |
| --- |
| Answer:  Use ‘ ps –eL’ to display the status of all process threads. An example of a command with multiple threads is:   1. Command: apache2 2. PID: 1234 3. TIDs: 1235, 1236 |

## Part F: Linux Process Management

Linux inter-process communication is based on signals, which are codes for well-defined messages sent to a process. The kill command sends a signal to a process. This command name is poor, because various signals can be sent, not just a SIGKILL signal.

1. Using the kill –l command, identify the code for each of the following terms, and then research and briefly describe the meaning of each.
   1. SIGKILL: (2 marks)

|  |
| --- |
| Answer:  Immediately terminates the process. The process cannot catch or ignore this signal. |

* 1. SIGTERM: (2 marks)

|  |
| --- |
| Answer:  Politely asks the process to terminate. The process can catch and handle this signal to perform cleanup before exiting. |

* 1. SIGSTOP: (2 marks)

|  |
| --- |
| Answer:  Stops (pauses) the process. The process cannot catch or ignore this signal. |

1. Run man ps, and then press CTRL-Z. What is the state of the process? (1 mark)

|  |
| --- |
| Answer:  The state of the process after pressing CTRL-Z is "Stopped" (T). |

CTRL-Z moved the man process to the background. It no longer controls the terminal window.

1. Run the jobs command. What is the purpose of this command? (1 mark)

|  |
| --- |
| Answer:  The ‘jobs’ command lists all jobs running in the current shell session, showing their status and job number. |

1. Run fg. What happens? Why? (1 mark)

|  |
| --- |
| Answer:  The ‘fg’ command brings a background job to the foreground, allowing it to interact with the terminal. |

1. Press CTRL-Z again to suspend the man ps process.
2. Run man proc, suspend the process using CTRL-Z and run jobs again.

You should now see two suspended man processes.

1. What command can you use to bring the man ps process to the foreground? (1 mark)

|  |
| --- |
| Answer:  Use the ‘fg %job\_number’ command to bring the ‘man ps’ process to the foreground. |

1. Press the **q** key to exit the man ps command.
2. Send the default kill signal (SIGTERM) to the man proc process using kill PID\_of\_man.
3. Run ps. Why is the process still listed? (Hint: the signal is NOT being ignored!) (1 mark)

|  |
| --- |
| Answer:  After sending the SIGTERM signal, the process may still be listed if it is performing cleanup or handling the termination request. It might not have exited immediately. |

1. Send the force kill signal (SIGKILL) to the man process using kill -9 PID\_of\_man.
2. Run ps, and then compare the results to the previous step. Explain what has occurred. (1 mark)

|  |
| --- |
| Answer:  Sending the SIGKILL signal (kill -9 PID\_of\_man) forces the process to terminate immediately. The process will no longer be listed in the process table, as it cannot handle or ignore this signal. |

# References

Process Explorer. (2023). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Process\_Explorer

# Resources

Silberschatz, A., Galvin, P.B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). John Wiley & Sons, Inc.

Erl, T., Mahmood, Z., & Puttini, R. (2013). *Cloud computing: Concepts, technology & architecture*. Prentice Hall.

Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2018). *Operating systems: Three easy pieces.* CreateSpace Independent Publishing Platform. <https://pages.cs.wisc.edu/~remzi/OSTEP/>