Lab 1- Process Information- Group 12

Testing

After running command “cat /proc/lab1” as a regular user, it was quickly noticed that there were no compilation errors, and output was printed to the terminal. The name of the process is "cat," meaning that the process which read the file is the "cat" command. The Process ID (PID) is the unique identifier assigned to the "cat" process and used by the kernel and the operating system to manage and track a process, which is different each time the code is run. The Parent Process ID (PPID) indicates the parent process of “cat” and is also unique for every time the code is run. The state shows “Running,” indicating that the process is currently executing. Finally, the real, effective, and saved UID and GID values are unique and correspond to their user account, indicating limited access to resources based on the permissions assigned to their user and group.

When the code is run as the root user, its real user ID and effective user ID are both set to zero as expected. This means that the process is running with the highest level of privilege and has the ability access any resource on the system. Similarly, the real group ID and effective group ID are zero for processes running as the root user. The root user can access system resources and files that are restricted to the root group.

Running the code “dd if/proc/lab1” command causes the process name to say “dd.” Using the “more /proc/lab1” command prints another unique PID and PPID, while having the process name “more.” Since both these commands were executed as a regular user, it makes sense that none of the UID and GID values printed zeros.

In summary, the difference in output is a result of the kernel module retrieving and displaying process information based on the identity and privileges of the process that reads the /proc/lab1 file. Regular users see information related to their own process, while the root user sees information related to the process that read the file but with superuser privileges. This is a fundamental aspect of Linux security and privilege separation.