Assignment – 4
==========

1. Which capabilities API(secccomp-bpf, AppArmor or SELinux) did you chose? Why did you make that choice?
-> We chose seccomp-bpf for our assignment. While using AppArmour or SElinux, we need to have a complete rule set beforehand that cover
s all behaviors an application may perform. If we missed out any system call in the rule set, we need to change our profiling again accordingly.
-> Seccomp-bpf is an intuitive approach especially for a developer because it allows application behaviour rules directly in the source code. Developer can easily allow or disallow as per the process functionality. In our case, client server application, we profiled our Parent and Child process of server and Client process using seccomp-bpf as per their respective functionalities and usage of system calls.

2.What was the process you used to ascertain the list of system calls required by each program?
We used strace and strace -f while running the executable to find the system calls which cause the program to get killed and added the required system calls accordingly.

3.What system calls are needed by each?
Server Program:

Server system-call list

- rt_sigreturn
- exit
- read
- write
- execve
- brk
- fstat
- open
- getpid
- access
- socket
- socketcall
- clone
- bind
- listen
- accept
- wait4 -exit_group

CHILD SPECIFIC CALLS

- mmap2
- munmap
- fstat64
- close
- mprotect
- set_thread_area
- prctl
- getcwd
- stat64
- mkdir
- chdir
- chroot
- setuid32
- getuid32

Client system-calls list

- rt_sigreturn
- exit
- read
- write
- fstat64
- socketcall
- exit_group

4.What happens when your application calls a prohibited syscall? what is the application behavior that results from the call?
-> The process gets called if the process attempts to call a prohibited syscall.
-> We tried adding fork() syscall in the child process of the Server program, since which was not in the seccomp-bpf allowed system call, the process got killed abruptly, while stracing we could see the fork() call which caused the process to get killed.