**Solution by using Bob the builder:**

We have written a python script that builds a custom Seccomp profile builder which will take the input of the list of commands from the user and block or deny the actions of those commands. Whenever an image is built using this seccomp enabled profile, the attacker cannot use harmful commands which can modify the settings or permissions of the host system. The name given to this application is “Bob the Builder”.

1. Implementation:
   1. Seccomp (Secure computation mode) Profile: Seccomp is a kernel feature offered by Linux. This feature is used to filter system calls. Using this feature, we have built a custom profile generator. [[1]](#endnote-1)
   2. Create\_json() function: In this function, a python dictionary is used to deploy a template profile. It takes commands that are inputted by the user as arguments and returns a custom profile that denies the actions of those commands.
2. Screenshots of working of Bob the Builder:
   1. Running the python script:

A screenshot of a computer

Description automatically generated

* 1. User enters the commands as an input:

A picture containing text, screenshot, monitor, computer

Description automatically generated

* 1. Denying the commands inputted by the user:

A picture containing text, screenshot, monitor, computer

Description automatically generated

1. S. Sultan, I. Ahmad and T. Dimitriou, "Container Security: Issues, Challenges, and the Road Ahead," in IEEE Access, vol. 7, pp. 52976-52996, 2019, doi: 10.1109/ACCESS.2019.2911732. [↑](#endnote-ref-1)