Problem statement-1 :

drop_tcp_port.py:

This program drops the tcp packets to the specified port(default 4040). The port can also be configured from the user space.

How it works:

- Loads and ebpf program that insects every incoming packet.
- Checks if the packet is a TCP packet.
- If the destination port matches the configured port, then the packet is dropped.
- The port number can be updated via a BPF map.

Requirements:

- Linux system with bpf support
- Python3
- BCC library should be installed.

Problem statement-2:

ebpf_filter.py:

This program allows traffic only at a specific TCP port (default 4040) for a given process name (for e.g, "myprocess"). All the traffic to all other ports for only that process will be dropped.

How it works:

- This program uses the psutil library to identify the process id of the specified process.
- An eBPF socket filter is loaded and attached to a network interface to monitor the traffic.
- The program contains a BPF map with the target process id and allowed port, enabling the eBPF code to identify packets originating from the specific process.
- If the packet originates from the specific process and is destined to the allowed port, then the packet is allowed.

- If the packet originates from the specific process and is destined to unallowed port, then the packet is dropped.

Requirements:

- Linux system (kernel 4.1 or higher)
- Python3 installed
- bcc library for python
- psutil library for python