Linux RT - Home Exercise @ Salt

Background

The following exercise goal is to test your ability to learn a new and exciting emerging technology !

The technology relevant for your role is eBPF. https://ebpf.io/

BPF (Berkeley Packet Filter) is a highly flexible and efficient virtual machine-like construct within the Linux kernel, enabling bytecode execution at various hook points securely. It is widely utilized across several Linux kernel subsystems, notably in networking, tracing, and security (e.g., sandboxing).

Although BPF has been around since 1992, this document focuses on the enhanced version, the Extended Berkeley Packet Filter (eBPF), which debuted in Kernel version 3.18. This modern iteration has effectively replaced the original, now termed "classic" BPF (cBPF). Historically, cBPF was recognized as the packet filtering language utilized by tools like tcpdump. However, in contemporary Linux systems, only eBPF is executed. When a classic BPF bytecode is loaded, it is automatically converted to eBPF format within the kernel before execution.

Exercise

- Create an eBPF program
- eBPF program should use Cilium/bcc frameworks
- eBPF program should be able to probe, using kprobes for both sys_read and sys_write kernel functions.
- The expected result:

  > Every time a call to sys_read and sys_write on the Linux machine it runs on, the eBPF program will print “hello sys_read/sys_write was called”

- Please provide the eBPF as well as the user plan code
- Please provide instructions for installation/running it.

Optional/Advantage

- Be able to pass configuration information from the user plan code to the eBPF program.
- Be able to pass some information from the eBPF program to the user plan code.

Once ready, we will set a meeting to discuss the implementation, we may ask some questions re why it was developed as it was as well as think together on possible improvements.

While the eBPF code is in C, the user plan code can be in the language of your choosing with an advantage to Go)

There are numerous tutorials and videos out there which can help in getting started. Feel free to use them.

Best of Luck !