Intrusion Detection/Prevention Systems

- Host-based Intrusion Detection Systems (IDS)
- Host-based Intrusion Prevention systems (IPS)

✓ Based on signatures (well known programs)

✓ Based on behaviors (unknown programs)

➡ Example : Syslog and Systrace on Linux

◉ Vulnerable to malicious programs residing in the kernel called "rootkits"

How to write better programs with unsafe programming languages?