null(2);
log(...);
null(-2);
null(3);
log(...);
null(-3);

Efficient Cont. Sensitive Intrusion Detection:
- null calls eliminate all ambiguity about stack and current function.

Objective:
- **Model of correct program behavior:**
  - Static analysis of binary code.
  - Construct an automaton modeling all system call sequences the program can generate.
- **Ensure execution does not violate model:**
  - use automaton to monitor system calls.
  - If automaton reaches an invalid state, then an intrusion attempt occurred.

Scenario 1:
Scenario 2:

null(2);
log(...);
null(-2);
nul(3);
log(...);
nul(-3);
nul(5);
log(...);
nul(-5);

Optimization:

Mimicry Attacks:
- Mimicry attacks attempt to evade system-call monitoring IDS by executing innocuous-looking sequences of system calls that accomplish the attacker's goals. Mimicry attacks may execute a sequence of dozens of system calls in order to evade detection.
- Attacker mimics correct behavior.
**Trojan:**
- Malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system.

**SandBoxes:**
- Goal: give untrusted programs limited rights.
- Principal of least privileges: requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user or a program on the basis of the layer we are considering) must be able to access only such information and resources that are necessary for its legitimate purpose.