Attack Surfaces Model

Natasha Kubiak

ECE 531, SUMMER 2022

DAEMON - SAMPLED.C

Variables:

#define:

DAEMON_NAME

OK

ERR_SETSID

ERROR

ERR_FORK

ERR_CHDIR

True

SIGTERM

SIGHUP

char

*ERROR_FORMAT

Functions

void _do_work(void)

void _signal_handler(const int signal)

- Int max size : 2147483647

Inputs

Signal:

SIGTERM:Terminated. A gentle kill that gives processes a chance to clean up.

SIGHUP:Hangup. Usually means that the controlling terminal has been disconnected.

Problems: Any unhandled signals simply returns to the log “unhandled signal”

Solution: Handle other signals, by closing log and exiting.

Standard input output are closed, no console.

close(STDIN_FILENO)

close(STDOUT_FILENO)

close(STDERR_FILENO)

Outputs

syslog

outputs to: var/log/messages , var/log/syslog

Problems:

- Large amounts of data to syslog can fill disk space.
- Logs are no longer saved when space is full, attacks would not leave a trail.

Solution

- Only listen on localhost to mitigate attack
- _do_work does not run indefinitely, will run for 100 seconds.