Single Process Application Example

Listing 1 shows event log record example for a single process application (scp) which handles tasks sequentially (i.e., does not spawn new process to handle new tasks).

Listing 1 Single process application example

(a) Scp Process Execve SYSCALL

```
type=SYSCALL TS=1618072037.116 ID=827810
syscall=execve exit=0 ppid=7162 pid=7176
exe="/usr/bin/scp"
type=EXECVE a0="scp" a1="/etc/hosts"
a2="x10@192.168.8.134:~/victim_data/hosts"
```

(b) Close SYSCALL

```
type=SYSCALL TS=1618072037.116 ID=827812
syscall=close ppid=7162 pid=7176
exe="/usr/bin/scp"
type=PROCTITLE TS=1618072037.116 ID=827812
proctitle="bash"
```