

## Kernel Module

The given kernel system call to get process details is implemented using module which is loaded via

- `insmod <module>.ko param=<process id>`

where process id is passed as input and <param> is defined as 'PID'

This module is unloaded using

- `rmmod <module>.ko`

The command `dmesg` is used to print output and see the process details

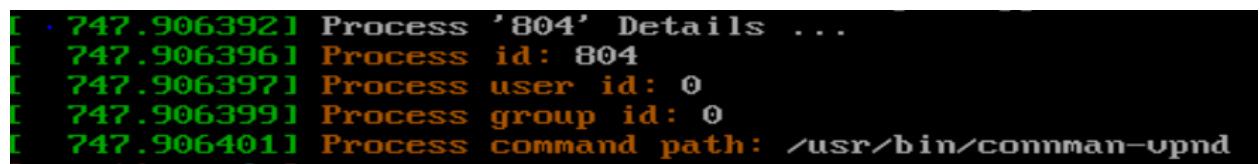
There are following details printed for the given PID

- Process id
- Process used id
- Process group id
- Process command path

For example, following are the commands used to get details for process id: 804

% `insmod processdetails.ko PID=804`

% `dmesg`



```
[ 747.906392] Process '804' Details ...  
[ 747.906396] Process id: 804  
[ 747.906397] Process user id: 0  
[ 747.906399] Process group id: 0  
[ 747.906401] Process command path: /usr/bin/commman-upnd
```

Details about the kernel module

1. The process id input is taken by defining a module\_param 'PID' of int type
  - `module_param(PID, int, <permissions>);`
2. The task\_struct for the given process id is fetched via following system call –
  - `get_pid_task(find_get_pid(PID),PIDTYPE_PID);`
3. The task\_struct has various fields to get information about process id, user id, group id and command path
  - Process id: `task_struct->pid`

- Process used id: `task_struct->real_cred->uid.val`
- Process group id: `taskp->real_cred->gid.val`
- Process command path: `task_struct->mm->exe_file->f_path`