

## KERNEL MODULE

First, I gave the module a license and then used it to initialize module\_param with the id initialized. After that I created a function named walter where I declared processes and using the process variable I printed Process name , UID , Group ID to the kernel.

After the walter function another function mike was created which was used to exit system call after printing every detail asked.

At last the module initialization and exit was done for the functions respectively.

```
[ 15.919426] elogind[820]: New session 1 of user drippy.
[ 5045.278629] kerlast: loading out-of-tree module taints kernel.
[ 5045.278656] kerlast: module verification failed: signature and/or required key missing - tainting kernel
[ 5045.278921] Process Name: su
[ 5045.278922] PID UID: 842 11 1000
[ 5045.278923] Group ID: 842
[ 6980.895371] watchdog: BUG: soft lockup - CPU#0 stuck for 1263s! [swapper/0:0]
[ 6980.899052] Modules linked in: kerlast(OE) 8021q garp stp mrp llc rfkill ufat fat crc10dif pclmul crc32_pclmul ghash_clmulni
intel_psmouse aesni_intel crypto_simd pcspkr e1000 cryptd mousedev intel_agp intel_gtt ext4 crc32c_generic crc16 mbcache jbd2 s
erio_raw atkbd libps2 uivaldi_fmap sr_mod cdrom i8042 crc32c_intel serio
[ 6980.899204] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G OE 5.19.9 #1 f0d7fae241d783aad123ec2675b226d43c90b356
[ 6980.899221] Hardware name: imnotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[ 6980.899228] RIP: 0010:native_safe_halt+0xb/0x10
[ 6980.899327] Code: 7e ff ff ff 7f 5b c3 65 48 8b 04 25 c0 bb 01 00 f0 80 48 02 20 48 8b 00 a8 08 74 82 eb c1 cc eb 07 0f 00 2d
a7 18 56 00 fb f4 <c3> 0f 1f 40 00 eb 07 0f 00 2d 97 18 56 00 f4 c3 cc cc cc cc cc 0f
[ 6980.899330] RSP: 0018:ffffffff82603e88 EFLAGS: 00000206
[ 6980.899335] RAX: 000000000002e2aa6 RBX: ffffffff826179c0 RCX: 0000000000000000
[ 6980.899340] RDX: 0000000000000002 RSI: ffffffff82482df1 RDI: ffffffff824b555e
[ 6980.899342] RBP: 0000000000000000 R08: 000007677e4f29be R09: 0000000000000000
[ 6980.899344] R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000
[ 6980.899346] R13: 0000000000000000 R14: ffffffff82617118 R15: 00000000db6c5cab
[ 6980.899350] FS: 0000000000000000(0000) GS:ffff88811bc00000(0000) knlGS:0000000000000000
[ 6980.899352] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 6980.899354] CR2: 0000564a521ad000 CR3: 00000001077b7000 CR4: 0000000000005060
[ 6980.899369] Call Trace:
[ 6980.899380] <TASK>
[ 6980.899386] default_idle+0xa/0x10
[ 6980.899397] default_idle_call+0x32/0xe0
[ 6980.899401] do_idle+0x1e1/0x1f0
[ 6980.899440] cpu_startup_entry+0x19/0x20
[ 6980.899444] rest_init+0xc0/0xc0
[ 6980.899454] arch_call_rest_init+0xa/0x10
[ 6980.899491] start_kernel+0x95b/0x980
[ 6980.899496] secondary_startup_64_no_verify+0xcd/0xdb
[ 6980.899506] </TASK>
[ 6980.900942] clocksource: timekeeping watchdog on CPU1: Marking clocksource 'tsc' as unstable because the skew is too large:
[ 6980.900972] clocksource: 'kvm-clock' wd_nsec: 1356067558883 wd_now: 65a2a6e3a4f wd_last: 51e6e81646c ma
sk: ffffffffffffffff
[ 6980.900978] clocksource: 'tsc' cs_nsec: 256556356514 cs_now: 12630abf3609 cs_last: ed12116490c mask: ff
fffffffffffffff
[ 6980.900983] clocksource: 'tsc' is current clocksource.
[ 6980.900988] tsc: Marking TSC unstable due to clocksource watchdog
[ 6980.902058] clocksource: Checking clocksource tsc synchronization from CPU 1 to CPUs 0.
[ 6980.902074] clocksource: Switched to clocksource kvm-clock
```