2018. 4. 19 금

과정 : TI, DSP, Xilinx Znq FPGA, MCU 기반의 프로그래밍 전문가 과정

Prof. 이상훈
gcccompil3r@gmail.com
Stu. 정상용
fstopdg@gmail.com

배운 내용.
1. Install screen
2. Monitor hacking & code 분석

1. How to install ‘screnn’
→ sudo apt-get install screen
execute
→ screen -a
Making another window : ctrl + ac
Changing the window : ctrl + aa

2. Monitor hacking
In the directory, kernel(from Homework)
→ make
→ insmod monito_hack.ko
Now, your monitor is hacked….

3. Driving(monitor_hack.c)
.vimrc : set up ‘glibc’
→ module_init(syscall_hooking_init)
→ First, drive the function ‘syscall_hooking_init’
CR0 분석…
write_cr0 분석...
kallsyms_lookup_name 분석...
set_memory_rw 분석...