```
CMPE 283 Assignment 1 Module Start
[  243.209850] Pinbased Controls MSR: 0x3f00000016
[  243.209852]   External Interrupt Exiting: Can set=Yes, Can clear=Yes
[  243.209853]   NMI Exiting: Can set=Yes, Can clear=Yes
[  243.209854]   Virtual NMIs: Can set=Yes, Can clear=Yes
[  243.209855]   Activate VMX Preemption Timer: Can set=No, Can clear=Yes
[  243.209855]   Process Posted Interrupts: Can set=No, Can clear=Yes
[  243.209857] Entry Controls MSR: 0xf3ff000011ff
[  243.209858]   Load debug controls: Can set=Yes, Can clear=No
[  243.209859]   IA-32e mode guest: Can set=Yes, Can clear=Yes
[  243.209860]   Entry to SMM: Can set=No, Can clear=Yes
[  243.209861]   Deactivate dual-monitor treatment: Can set=No, Can clear=Yes
[  243.209861]   Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[  243.209862]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[  243.209863]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[  243.209863]   Load IA32_BNDCFGS: Can set=No, Can clear=Yes
[  243.209864]   Conceal VMX from PT: Can set=No, Can clear=Yes
[  243.209865]   Load IA32_RTIT_CTL: Can set=No, Can clear=Yes
[  243.209866]   Load CET state: Can set=No, Can clear=Yes
[  243.209867] Exit Controls MSR: 0x3fffff00036dff
[  243.209868]   Save debug controls: Can set=Yes, Can clear=No
[  243.209869]   Host address-space size: Can set=Yes, Can clear=Yes
[  243.209870]   Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[  243.209870]   Acknowledge interrupt on exit: Can set=Yes, Can clear=Yes
[  243.209871]   Save IA32_PAT: Can set=Yes, Can clear=Yes
[  243.209872]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[  243.209872]   Save IA32_EFER: Can set=Yes, Can clear=Yes
[  243.209873]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[  243.209874]   Save VMX-preemtion time value: Can set=No, Can clear=Yes
[  243.209874]   Clear IA32_BNDCFGS: Can set=No, Can clear=Yes
[  243.209875]   Conceal VMX from PT: Can set=No, Can clear=Yes
[  243.209876]   Clear IA32_RTIT_CTL: Can set=No, Can clear=Yes
[  243.209876]   Load CET state: Can set=No, Can clear=Yes
[  243.209878] Processor based Controls MSR: 0xfff9fffe0401e172
[  243.209879]   Interrupt-window exiting: Can set=Yes, Can clear=Yes
[  243.209880]   Use TSC offsetting: Can set=Yes, Can clear=Yes
[  243.209881]   HLT exiting: Can set=Yes, Can clear=Yes
[  243.209881]   INVLPG exiting: Can set=Yes, Can clear=Yes
[  243.209882]   MWAIT exiting: Can set=Yes, Can clear=Yes
[  243.209883]   RDMPC exiting: Can set=Yes, Can clear=Yes
[  243.209883]   RDTSC exiting: Can set=Yes, Can clear=Yes
[  243.209884]   CR3-load exiting: Can set=Yes, Can clear=No
[  243.209885]   CR3-store exiting: Can set=Yes, Can clear=No
[  243.209885]   CR8-load exiting: Can set=Yes, Can clear=Yes
[  243.209886]   CR8-store exiting: Can set=Yes, Can clear=Yes
[  243.209887]   Use TPR shadow: Can set=Yes, Can clear=Yes
[  243.209887]   MOV-DR exiting: Can set=Yes, Can clear=Yes
[  243.209888]   Unconditional I/O exiting: Can set=Yes, Can clear=Yes
[  243.209889]   Use I/O bitmaps: Can set=Yes, Can clear=Yes
[  243.209889]   Monitor trap flag: Can set=Yes, Can clear=Yes
[  243.209890]   Use MSR bitmaps: Can set=Yes, Can clear=Yes
[  243.209891]   Monitor exiting: Can set=Yes, Can clear=Yes
[  243.209891]   PAUSE exiting: Can set=Yes, Can clear=Yes
[  243.209892]   Activate secondary controls: Can set=Yes, Can clear=Yes
[  243.209894] Secondary Processor based Controls MSR: 0x553cfe00000000
[  243.209895]   Virtualize APIC accessories: Can set=No, Can clear=Yes
[  243.209895]   Enable EPT: Can set=Yes, Can clear=Yes
[  243.209896]   Descriptor-table exiting: Can set=Yes, Can clear=Yes
[  243.209896]   Enable RDTSCP: Can set=Yes, Can clear=Yes
[  243.209897]   Virtualize x2APIC mode: Can set=Yes, Can clear=Yes
[  243.209898]   Enable VPID: Can set=Yes, Can clear=Yes
[  243.209898]   WBINVD exiting: Can set=Yes, Can clear=Yes
[  243.209899]   Unrestricted guest: Can set=Yes, Can clear=Yes
[  243.209900]   APIC-register virtualization: Can set=No, Can clear=Yes
[  243.209900]   Virtual-interrupt delivery: Can set=No, Can clear=Yes
[  243.209901]   PAUSE-loop exiting: Can set=Yes, Can clear=Yes
[  243.209902]   RDRAND exiting: Can set=Yes, Can clear=Yes
[  243.209902]   Enable INVPCID: Can set=Yes, Can clear=Yes
[  243.209903]   Enable VM functions: Can set=Yes, Can clear=Yes
[  243.209904]   VMCS shadowing: Can set=No, Can clear=Yes
[  243.209904]   Enable ENCLS exiting: Can set=No, Can clear=Yes
[  243.209905]   RDSEED exiting: Can set=Yes, Can clear=Yes
[  243.209906]   Enable PML: Can set=No, Can clear=Yes
[  243.209907]   EPT-violation #VE: Can set=Yes, Can clear=Yes
[  243.209907]   Conceal VMX from PT: Can set=No, Can clear=Yes
[  243.209908]   Enable XSAVES/XRSTORS: Can set=Yes, Can clear=Yes
[  243.209909]   Mode-based execute control for EPT: Can set=Yes, Can clear=Yes
[  243.209909]   Sub-page write permissions for EPT: Can set=No, Can clear=Yes
[  243.209910]   Intel PT uses guest physical addresses: Can set=No, Can clear=Yes
[  243.209911]   Use TSC scaling: Can set=No, Can clear=Yes
[  243.209912]   Enable user wait and pause: Can set=No, Can clear=Yes
[  243.209912]   Enable ENCLV exiting: Can set=No, Can clear=Yes
```