# CMPE283

work done by Aishwarya

**Git link:https://github.com/Aishwaryasjsu/CMPE283\_Assignment.git**

\*\*\*\*\*\*\*\*\*\*\*\*\* **Created Instance in vm from gcp UI**. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

with machine configuration as :

Machine type n2-standard-2

CPU platform Intel Cascade Lake

Architecture x86/64

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* **Executed following commands on console** \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

gcloud compute instances export instance-10 \

--destination=cmpe283-1.yaml \

--zone=us-central1-a

enabled virtualisation =true in cmpe283-1.yaml

advancedMachineFeatures:

enableNestedVirtualization: true

gcloud compute instances update-from-file instance-10 \

--source=cmpe283-1.yaml \

--most-disruptive-allowed-action=RESTART \

--zone=us-central1-a

\*\*\*\*\*\*\*\*\*\*\*\*\* **Created folder :cmpe283-1** \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

files created 1. Make file

2. cmpe283-1.c

for IA32\_VMX\_PINBASED\_CTLS 0x481

IA32\_VMX\_PROCBASED\_CTLS 0x482

IA32\_VMX\_EXIT\_CTLS 0x483

IA32\_VMX\_ENTRY\_CTLS 0x484

IA32\_VMX\_PROCBASED\_CTLS2 0x48B

IA32\_VMX\_PROCBASED\_CTLS3 0x492

\*\*\*\*\*\*\*\* **Executed following commands** :\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#make

sudo bash

apt install gcc make

Exit

#sudo apt install linux-headers-$(uname -r)

uname -r

sudo apt install linux-headers-5.4.0-1092-gcp

Make

sudo insmod ./cmpe283-1.ko

Sudo dmesg

**\*\*\*\*\*\*\*\*OUTPUT\*\*\*\*\*\*\*\***

[ 301.254262] CMPE 283 Assignment 1 Module Start

[ 301.254264] Pinbased Controls MSR: 0x3f00000016

[ 301.254265] External Interrupt Exiting: Can set=Yes, Can clear=Yes

[ 301.254265] NMI Exiting: Can set=Yes, Can clear=Yes

[ 301.254266] Virtual NMIs: Can set=Yes, Can clear=Yes

[ 301.254266] Activate VMX Preemption Timer: Can set=No, Can clear=Yes

[ 301.254267] Process Posted Interrupts: Can set=No, Can clear=Yes

[ 301.254269] Procbased Controls MSR: 0xf7b9fffe0401e172

[ 301.254270] Interrupt Window Exiting: Can set=Yes, Can clear=Yes

[ 301.254270] Use TSC Offsetting: Can set=Yes, Can clear=Yes

[ 301.254271] HLT Exiting: Can set=Yes, Can clear=Yes

[ 301.254271] INVLPG Exiting: Can set=Yes, Can clear=Yes

[ 301.254271] MWAIT Exiting: Can set=Yes, Can clear=Yes

[ 301.254272] RDPMC Exiting: Can set=Yes, Can clear=Yes

[ 301.254272] RDTSC Exiting: Can set=Yes, Can clear=Yes

[ 301.254273] CR3 Load Exiting: Can set=Yes, Can clear=No

[ 301.254273] CR3 Store Exiting: Can set=Yes, Can clear=No

[ 301.254274] Activate Tertiary Controls: Can set=No, Can clear=Yes

[ 301.254274] CR8 Load Exiting: Can set=Yes, Can clear=Yes

[ 301.254275] CR8 Store Exiting: Can set=Yes, Can clear=Yes

[ 301.254275] Use TPR Shadow: Can set=Yes, Can clear=Yes

[ 301.254276] NMI Window Exiting: Can set=No, Can clear=Yes

[ 301.254276] MOV-DR Exiting: Can set=Yes, Can clear=Yes

[ 301.254277] Unconditional I/O Exiting: Can set=Yes, Can clear=Yes

[ 301.254277] Use I/O Bitmaps: Can set=Yes, Can clear=Yes

[ 301.254278] Monitor Trap Flag: Can set=No, Can clear=Yes

[ 301.254278] Use MSR Bitmaps: Can set=Yes, Can clear=Yes

[ 301.254279] MONITOR Exiting: Can set=Yes, Can clear=Yes

[ 301.254279] PAUSE Exiting: Can set=Yes, Can clear=Yes

[ 301.254279] Activate Secondary Controls: Can set=Yes, Can clear=Yes

[ 301.254281] Secondary Procbased Controls MSR: 0x51ff00000000

[ 301.254282] Virtualize APIC accesses: Can set=Yes, Can clear=Yes

[ 301.254282] Enable EPT: Can set=Yes, Can clear=Yes

[ 301.254283] Descriptor Table Exiting: Can set=Yes, Can clear=Yes

[ 301.254283] Enable RDTSCP: Can set=Yes, Can clear=Yes

[ 301.254284] Virtualize x2APIC Mode: Can set=Yes, Can clear=Yes

[ 301.254285] Enable VPID: Can set=Yes, Can clear=Yes

[ 301.254285] WBINVD Exiting: Can set=Yes, Can clear=Yes

[ 301.254286] Unrestricted Guest: Can set=Yes, Can clear=Yes

[ 301.254286] APIC-register Virtualization: Can set=Yes, Can clear=Yes

[ 301.254287] Virtual-interrupt Delivery: Can set=No, Can clear=Yes

[ 301.254287] PAUSE-loop Exiting: Can set=No, Can clear=Yes

[ 301.254288] RDRAND exiting: Can set=No, Can clear=Yes

[ 301.254288] Enable INVPCID: Can set=Yes, Can clear=Yes

[ 301.254289] Enable VM Functions: Can set=No, Can clear=Yes

[ 301.254289] VMCS Shadowing: Can set=Yes, Can clear=Yes

[ 301.254290] Enable ENCLS Exiting: Can set=No, Can clear=Yes

[ 301.254290] RDSEED Exiting: Can set=No, Can clear=Yes

[ 301.254290] Enable PML: Can set=No, Can clear=Yes

[ 301.254291] EPT-violation #VE: Can set=No, Can clear=Yes

[ 301.254291] Conceal VMX from PT: Can set=No, Can clear=Yes

[ 301.254292] Enable XSAVES/XRSTORS: Can set=No, Can clear=Yes

[ 301.254292] Mode-based Execute Control for EPT: Can set=No, Can clear=Yes

[ 301.254293] Sub-page Write Permissions for EPT: Can set=No, Can clear=Yes

[ 301.254293] Intel PT Uses Guest Physical Addresses: Can set=No, Can clear=Yes

[ 301.254294] Use TSC Scaling: Can set=No, Can clear=Yes

[ 301.254294] Enable User Wait and Pause: Can set=No, Can clear=Yes

[ 301.254295] Enable ENCLV Exiting: Can set=No, Can clear=Yes

[ 301.254297] Exit Controls MSR: 0x3fefff00036dff

[ 301.254297] Save Debug Controls: Can set=Yes, Can clear=No

[ 301.254298] Host Addres-Space Size: Can set=Yes, Can clear=Yes

[ 301.254298] Load IA32\_PERF\_GLOBAL\_CTRL: Can set=No, Can clear=Yes

[ 301.254299] Acknowledge Interrupt On Exit: Can set=Yes, Can clear=Yes

[ 301.254299] Save IA32\_PAT: Can set=Yes, Can clear=Yes

[ 301.254299] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 301.254300] Save IA32\_EFER: Can set=Yes, Can clear=Yes

[ 301.254300] Load IA32\_EFER: Can set=Yes, Can clear=Yes

[ 301.254301] Save VMXpreemption Timer Value: Can set=No, Can clear=Yes

[ 301.254301] Clear IA32\_BNDCFGS: Can set=No, Can clear=Yes

[ 301.254302] Conceal VMX from PT: Can set=No, Can clear=Yes

[ 301.254302] Clear IA32\_RTIT\_CTL: Can set=No, Can clear=Yes

[ 301.254303] Clear IA32\_LBR\_CTL: Can set=No, Can clear=Yes

[ 301.254303] Load CET state: Can set=No, Can clear=Yes

[ 301.254304] Load PKRS: Can set=No, Can clear=Yes

[ 301.254304] Activate Secondary Controls: Can set=No, Can clear=Yes

[ 301.254306] Entry Controls MSR: 0xd3ff000011ff

[ 301.254306] Load Debug Controls: Can set=Yes, Can clear=No

[ 301.254307] IA-32e Mode Guest: Can set=Yes, Can clear=Yes

[ 301.254307] Entry to SMM: Can set=No, Can clear=Yes

[ 301.254308] Deactivate Dual Monitor Treatment: Can set=No, Can clear=Yes

[ 301.254308] Load IA32\_PERF\_GLOBAL\_CTRL: Can set=No, Can clear=Yes

[ 301.254309] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 301.254309] Load IA32\_EFER: Can set=Yes, Can clear=Yes

[ 301.254310] Load IA32\_BNDCFGS: Can set=No, Can clear=Yes

[ 301.254310] Conceal VMX from PT: Can set=No, Can clear=Yes

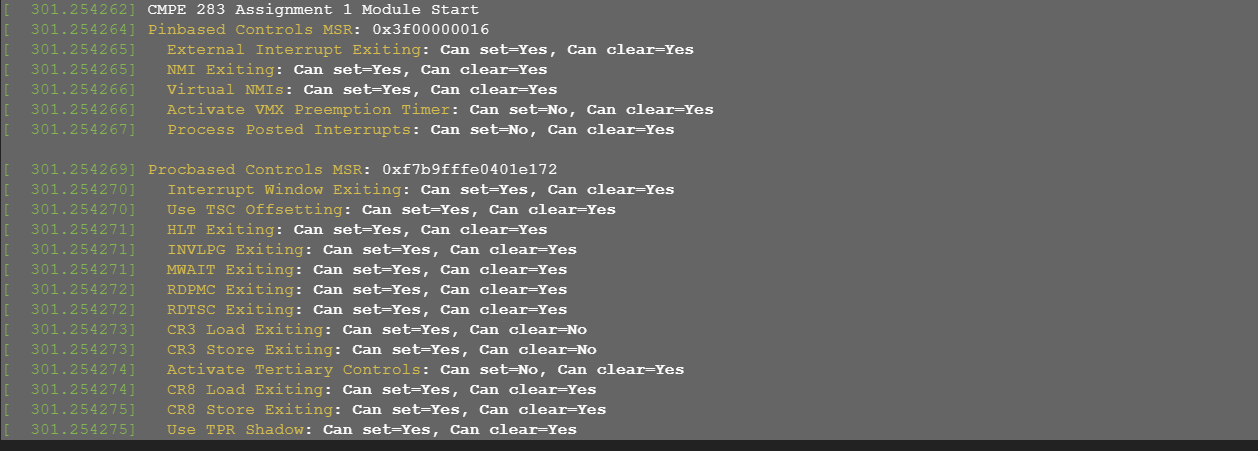
[ 301.254311] Load IA32\_RTIT\_CTL: Can set=No, Can clear=Yes

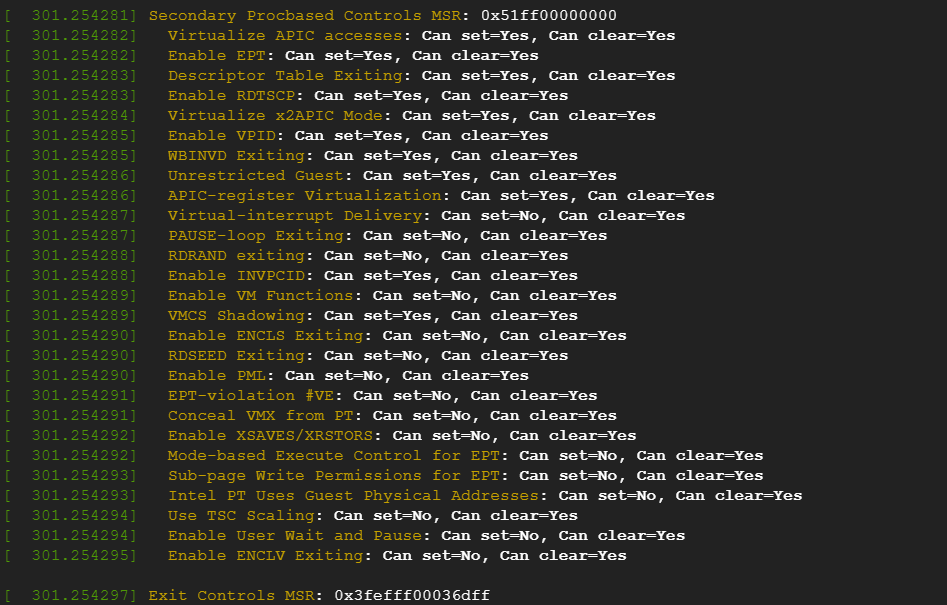
[ 301.254311] Load CET State: Can set=No, Can clear=Yes

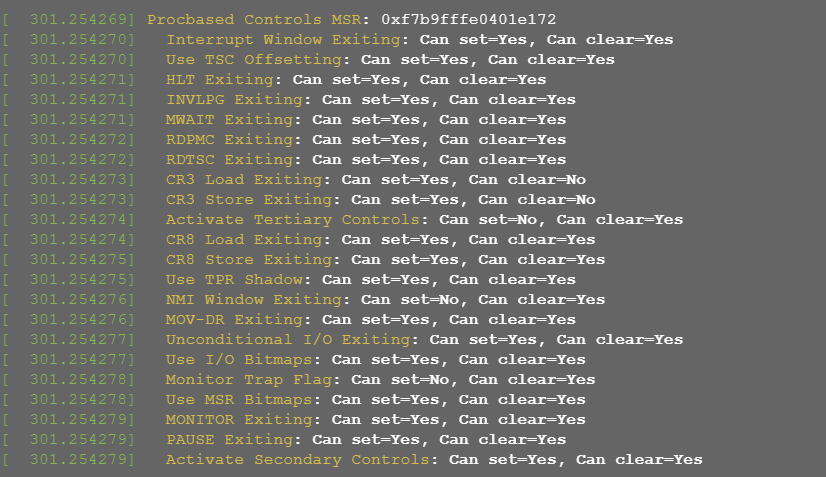
[ 301.254312] Load Guest IA32\_LBR\_CTL: Can set=No, Can clear=Yes

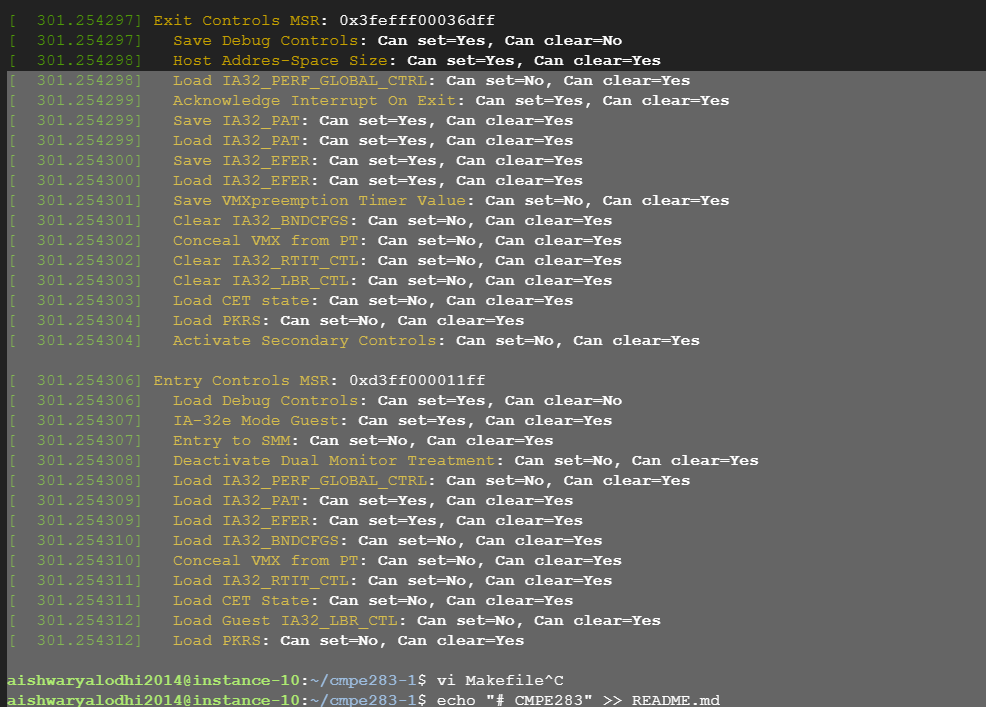
[ 301.254312] Load PKRS: Can set=No, Can clear=Yes

Screenshot :









Nisha \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Git link:https://github.com/nisha-sjsu/cmpe283-assignment1/tree/master