CSC427H5 2020 Tutorial: Meltdown and Spectre

Setup VM:

```
$ mkdir /virtual/UTORID
$ cd /virtual/UTORID
$ cp -r /virtual/csc427/kali .
```

USERNAME: root
PASSWORD: toor

Check the Meltdown and Spectre vulnerabilities:

Open kali command line

```
$ cd Desktop
$ git clone https://github.com/speed47/spectre-meltdown-checker.git
$ cd spectre-meltdown-checker
$ ./spectre-meltdown-checker.sh --explain
```

1. Copy the Kernel and CPU versions and the check SUMMARY into the file answer.txt

Close patches:

First of all, we need to close KALSR.
Because if we keep KALSR on, the POC code we are going to run may cost larger amount of time.
Also we need to diable some patches.

```
$ grep GRUB_CMDLINE_LINUX_DEFAULT /etc/default/grub
$ sudo vim /etc/default/grub
```

Find the line of GRUB_CMDLINE_LINUX_DEFAULT and set

```
GRUB_CMDLINE_LINUX_DEFAULT = "quiet nokaslr noibrs noibpb nopti nospectre_v2 nospectre_v1 l1tf=off nospec_store_bypass_disable no_stf_barrier mds=off mitigations=off"
```

```
$ grep quiet /etc/default/grub
$ sudo update-grub
```

2. Put the document “grub” which is “/etc/default/grub” with answer.txt together, it will be included in submit zip.

   Then reboot the VM

   ```
   $ shutdown -r now
   ```

   Do spectre and meltdown check again:

   ```
   $ cd Desktop/spectre-meltdown-checker
   $ ./spectre-meltdown-checker.sh --explain
   ```

3. See what’s different in SUMMARY, copy and paste the SUMMARY into the answer.txt

   Now, you can see what did GRUB_CMDLINE_LINUX_DEFAULT = "quiet nokaslr noibrs noibpb nopti nospectre_v2 nospectre_v1 l1tf=off nospec_store_bypass_disable no_stf_barrier mds=off mitigations=off" do.

4. Do an one sentence explain in answer.txt

   Try some Meltdown Proof-of-Concpet(POC) code:

   ```
   $ cd /root/Destop
   $ git clone https://github.com/IAIK/meltdown.git
   $ cd meltdown
   $ make
   $ taskset 0x1 ./test
   ```

5. Save the result of the output in answer.txt

   Try some Spectre Proof-of-Concpet(POC) code:

   ```
   $ cd /root/Destop
   $ git clone https://github.com/crozone/SpectrePoC.git
   $ cd SpectrePoC
   $ make
   $ ./spectre.out
   ```

   What’s the secert sentence you got?

6. Copy the whole output into the answer.txt

Open spectre.c
change the char * secret to another different sentence(you can write want you want)

```
$ make clean
$ make
$ ./spectre.out
```

See if you get the secret you wrote.

7. Copy the whole output into the answer.txt

Then let’s build a version with Linux kernel array_index_mask_nospec() mitigation included

```
$ make clean
$ CFLAGS=-DLINUX_KERNEL_MITIGATION make
$ ./spectre.out
```

Can you still got the secret?

8. Answer YES or NO and put the whole output into the answer.txt

SUBMITION:

submit one zip, which named meltdown.zip
this zip include two documents: grub, answer.txt
answer.txt should be in the format below:

```
Q1:
…
Q2:
…
Q3:
…
Q4:
.
.
.
Q8:
…
```

Submit the zip through UTM Submit.