CSIE 5310 Assignment 3 (Due on November 20th 14:10)

In this assignment, you will test pKVM's VM protection capability.

0. Late submission policy

- 1 pt deduction for late submissions within a day (before Nov. 21st 14:10)
- 2 pts deduction for late submissions within 2 days (before Nov. 22nd 14:10)
- zero points for submissions delayed by more than 2 days.

1. Before you start

- As in Assignment 1, you should prepare a working Ubuntu environment, which you are allowed to install any software packages as you wish. We recommend installing Ubuntu on a VM (on VMWare workstation/fusion or parallel), or on a bare-metal machine (laptop or lab server) that you have full control. The tutorial provided as follows is based on Ubuntu 22.04 LTS. Please make sure to have at least 50GB free storage in your Ubuntu environment.
- Download the file `vm_hw3_files.zip` from this link and unzip it. The unzipped folder contains 3 files, which are used in this assignment:
  - `pkvm_host_Image`
  - `run-pkvm.sh`
  - `cloud.img`

2. Run pKVM's host

To test pKVM, you need to launch pKVM's host first. Please follow the instructions below.

Compile QEMU

> You can skip this step if you still have the QEMU setup from Assignment 1 on your system.

Clone QEMU from the repo and checkout to version `v7.0.0`:

```
# git clone https://gitlab.com/qemu-project/qemu.git
# cd qemu/
# git checkout tags/v7.0.0
```

Then configure and compile qemu from the source. You may run into some errors when you do the `configure` command, this is normally because you have missing packages. Google will be your friend for addressing the errors.

```
# cd qemu
# ./configure --target-list=aarch64-softmmu --disable-werror
# make -j4 (-j is to compile in parallel)
# sudo make install
```

Run pKVM's Host

After the compilation of QEMU, let's run pKVM's host. Execute the following command to launch pKVM's host.

```
# ./run-pkvm.sh -k $PATH_TO_pkvm_host_Image -i $PATH_TO_cloud.img
```

3. Run a VM in pKVM's Host

We have set up the virtual disk image of pKVM's host so that you can easily launch a VM. After you launch pKVM's host, you will see the following files in the `/root` directory.

- `cloud-inner.img`: the virtual disk image of the VM.
- `Image`: the kernel image of the VM.
- `run-guest.sh`: the script to launch the VM.

Execute the following command to launch a VM.

```
# ./run-guest.sh -k Image -i cloud-inner.img
```

4. Test pKVM

Now, you are able to launch a VM on pKVM's host and test pKVM. As introduced in the class, pKVM prevents the host Linux from accessing the VM's memory.

You are tasked to validate this protection. Come up with **one** methodology to access the VM's memory from pKVM's host.

You **are not allowed to** modify QEMU (the host and guest), pKVM, the VM's kernel image (i.e., `Image`) or its virtual disk image (i.e., `cloud_inner.img`).

Bonus

You will get extra points if you provide an additional distinct methodology to access the VM's memory from pKVM's host.

5. Grading

You need to submit a write-up and a video recording. The requirements are detailed below.

Write-up (5pts)

The write-up must include:

- A step-by-step explanation of how you test pKVM.
- The resulting behaviors of pKVM's host.

Video Recording (5pts)

The video recording should capture the entire procedure of running your test, including the resulting behaviors of pKVM's host.

Bonus (2pts)

If you provide an additional distinct methodology to access the VM's memory from pKVM's host, please include it in your write-up and the recording.

6. Submission

You should submit the assignment via NTU Cool. You are required to submit the following files. Replace `[Student-ID]` with your student number. For example, if your student number is `r01234567`, then `[Student-ID]` should be `r01234567`.

- `write-up.pdf`: the write-up file.
- `[Student-ID]_hw3.mp4`: the video recording.

Please place those files into a folder named `[Student-ID]_hw3`. The folder structure should be the same as follows.

```
[Student-ID]_hw3
|---- write-up.pdf
└---- [Student-ID]_hw3.mp4
```

Then, compress the folder into `[Student-ID]_hw3.zip` and submit it to NTU Cool.