# 2024 NTU Virtual Machine HW2 Writeup

**StudentID : R12922054**

## *[Instructions on compiling your kernel module.]*

- make KDIR=/PATH/TO/LINUX ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu-

## *[Explanations of how your code works, including the kernel module, kernel patch, and QEMU patch (if you modified QEMU).]*

### Kernel Module

There are two steps to implement the kernel module.

1. The first is initializing the mapping between the MMIO physical address and the MMIO virtual address. After I use the function API, `ioremap`, to make the physical address translate to the virtual address, I get the virtual address of `0x0x0b000000` and `0x0b000001`.
2. The second is completing the function, `virt_walker_read` and `virt_walker_write`. The important thing I do is use the function APIs, `ioread8`, `copy_from_user` and `iowrite8`.
   - Using `ioread8(the virtual address of 0x0x0b000001)` to Get the SEEK value in the function `virt_walker_read`.
   - In the function `virt_walker_write`, the first thing I do is use `copy_from_user` to get the value I want to store in the HIDE register. After that, I use `iowrite8(hide_value, the virtual address of 0x0x0b000000)` to write the value to the HIDE register.

### Kernel Patch

I modified the file, `arch/arm64/kvm/mmio.c`. The implementation steps are as follows.

1. Judge that the MMIO physical address is `0x0b000000` or `0x0b000001`.
2. If yes, start to
   - While doing the HIDE operation, implement walking `stage-2 page table` to get the leaf entry that maps GPA `0x40000000` and store the value to bit [58:51] of the leaf stage-2 page table entry.
   - While doing the SEEK operation, implement walking `stage-2 page table` to get the leaf entry that maps GPA `0x40000000` and return the value in bit [58:51] of the leaf stage-2 page table entry.

   All of my stage-2 page table walking implementation is based on the functions kvm_pgtable_get_leaf and leaf_walker in /arch/arm64/kvm/hyp/pgtable.c, along with guidance from the resource at this website [1]
3. Ultimately, I performed bitwise operations to either store a value in bits [58:51] of the leaf stage-2 page table entry mapping GPA 0x40000000 upon locating the entry, or to retrieve the value from bits [58:51] of this entry when found.

## References

[1] "KVM ARM: new page table walker," [Online]. Available: https://rhythm16.github.io/kvm_pgtable/#kvm-pgtable-walk