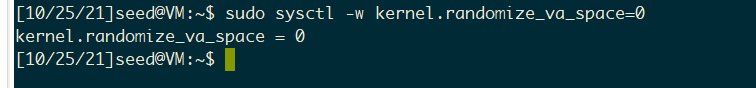
2.1 Turning Off Countermeasures

2.2.1 Address Space Randomization

$ sudo sysctl -w kernel.randomize\_va\_space=0



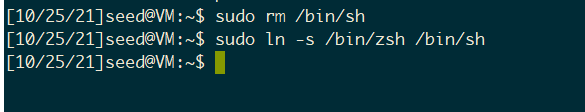
2.2.2 The StackGuard Protection Scheme

2.2.3 Non-Executable Stack

2.2.4 Configuring /bin/sh

$ sudo rm /bin/sh

$ sudo ln -s /bin/zsh /bin/sh



According to 2.2.2 and 2.2.3, we know that it is necessary to use command

$ gcc -fno-stack-protector -z execstack example.c -o example

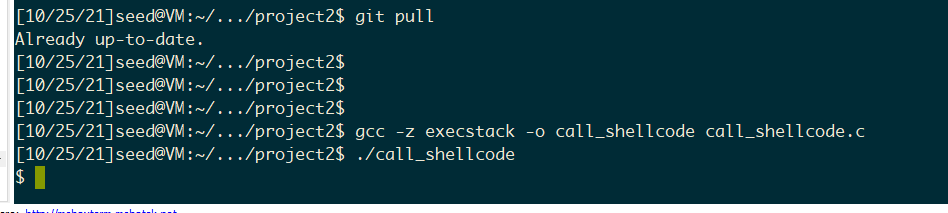
instead of

$ gcc example.c -o example

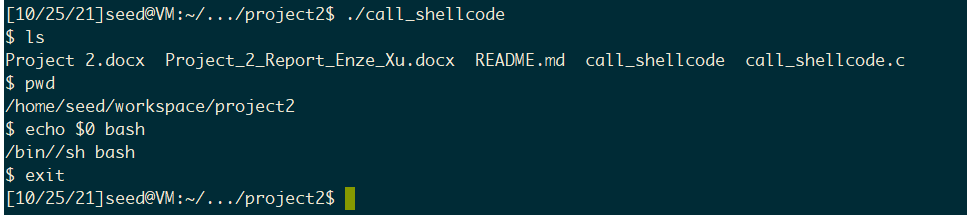
at our later steps.

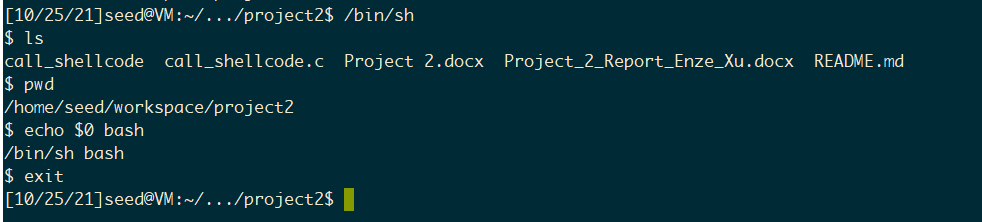
2.2 Task 1: Running Shellcode

**Execution:**



**Description:**



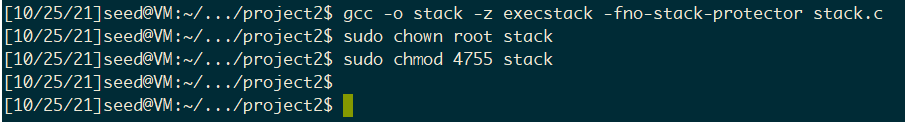


After executing “./call\_shellcode”, I successfully invoked “/bin/sh” as if I called “/bin/sh” in the shell directly.

2.3 The Vulnerable Program

**Execution:**

Compile it, change the ownership, and then change the permission.

****

2.4 Task 2: Exploiting the Vulnerability