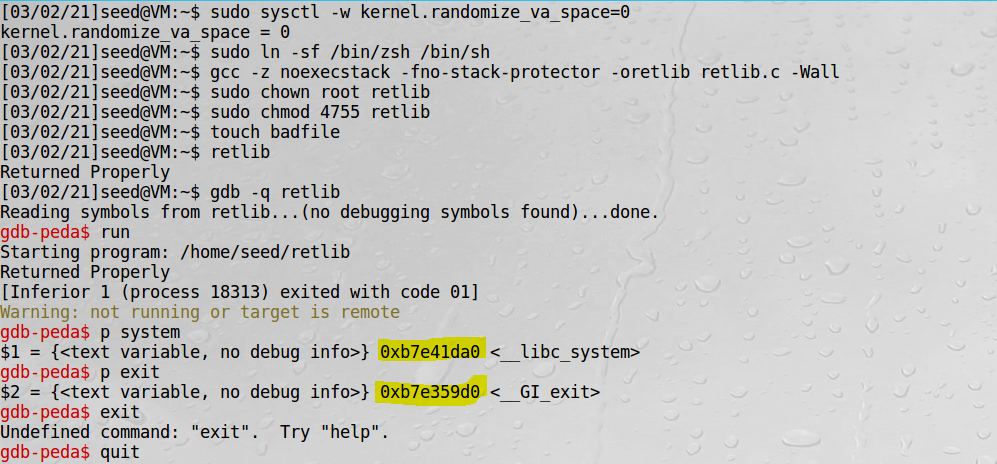
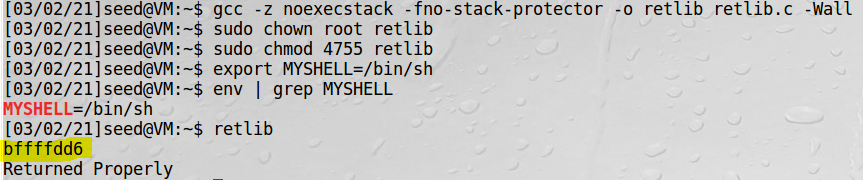
Connor Bradt

**Task 1**



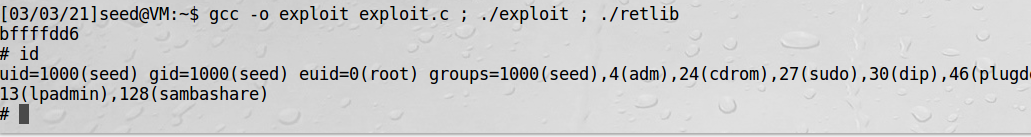
Found libc addresses.

**Task 2**



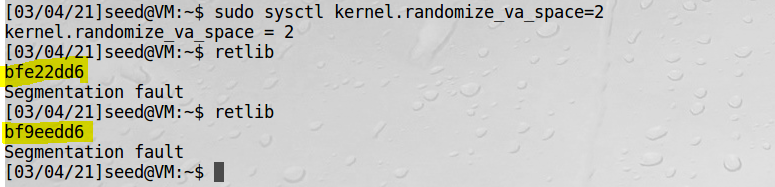
Found “/bin/sh” address.

**Task 3**



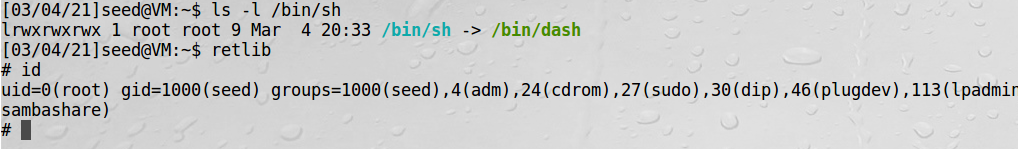
Root shell accessed. If I change the name length of “retlib.c” this attack will not work because it will change the “/bin/sh” address.

**Task 4**



Cannot access root shell because **“bin/sh” address** changes with each execution indicated by the highlighted addresses.

**Task 5 (Bonus)**



Used “setuid(0);” in “retlib.c” code to work around “/bin/dash” countermeasure to get the root shell.

Git clone “repository URL”

Change directory(cd) to remote repository folder

Git remote add “name” “repository URL”

\*create folder to copy the files to.

Change directory(cd ..) until home.

cp path/local\_repo/src/\* path/remote\_repo/src ( easier to copy paths from home directory)

Change directory(cd) to remote repository folder

git rm --cached directory

git add directory (to avoid the git submodule issue. {may not be needed})

git add local\_repo/src/\* (done in remote repository folder)

git commit –m “local files”

git push origin(“remote name”) master

Try git fetch or git pull to get the extra report documents into the remote repository