Eric Pereira and Dmitri Piquero

Lab 13

CSE3120

28 November 2018

CTF 2



HEXDUMP:

0000000 db9b 50e3 04df 9b24 3dd9 0000 0000 8166

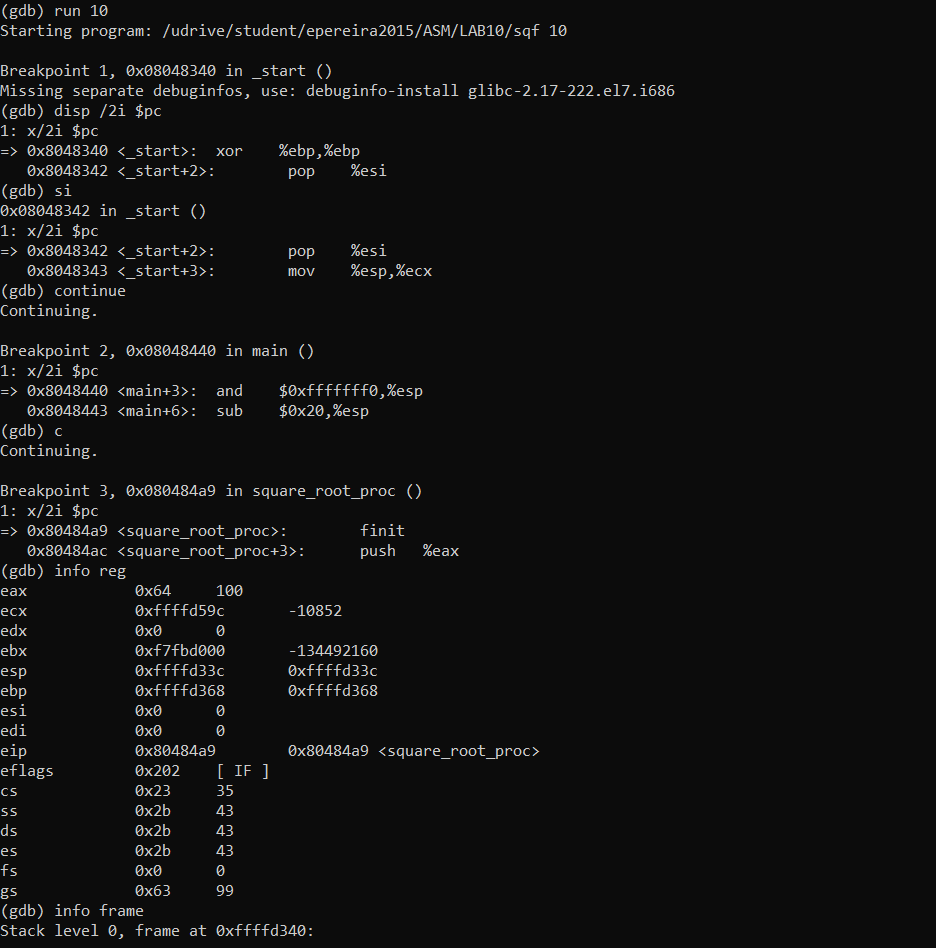
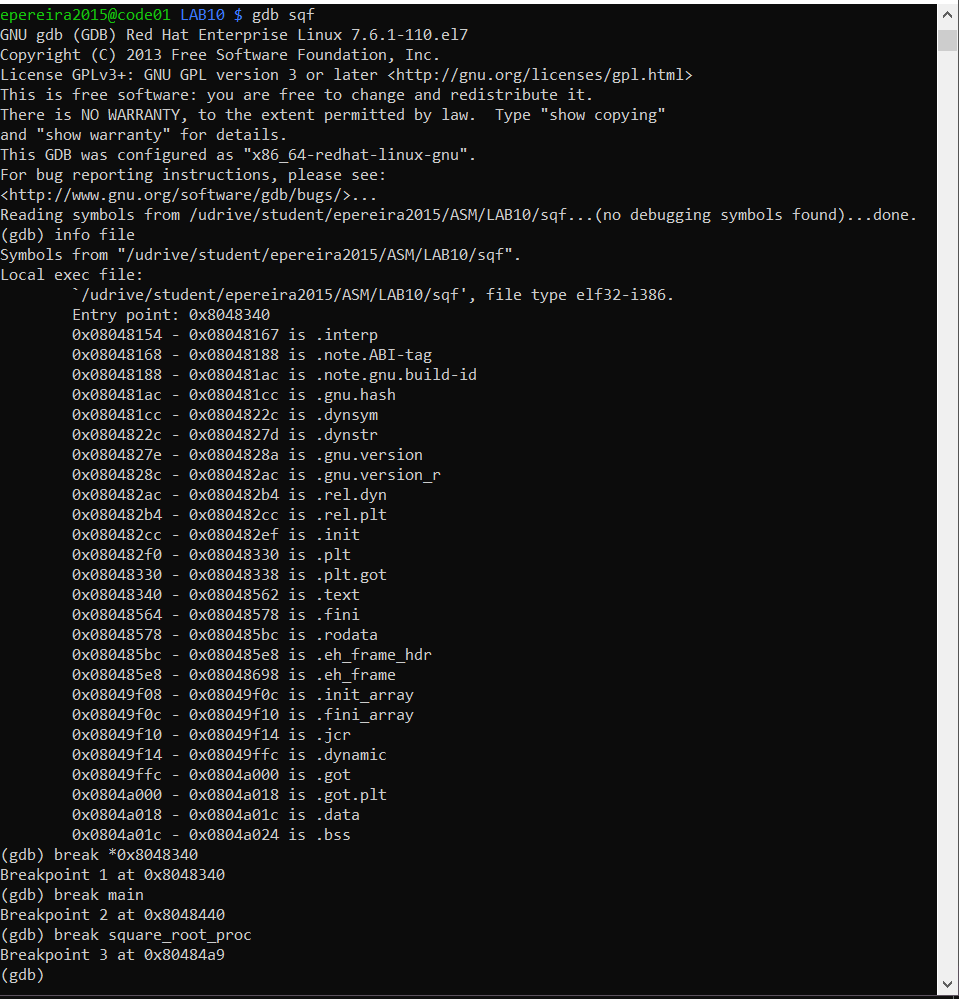
0000010 000d 0000 0000 d90c 002d 0000 d900 dffa

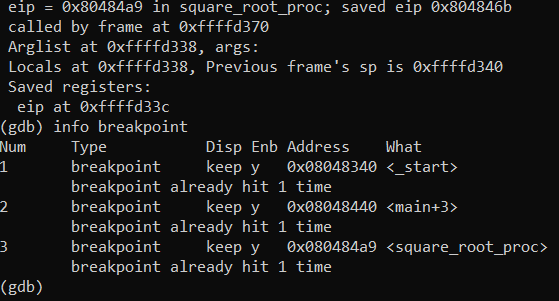
0000020 241c 9b58 3dd9 0000 0000 8166 0025 0000

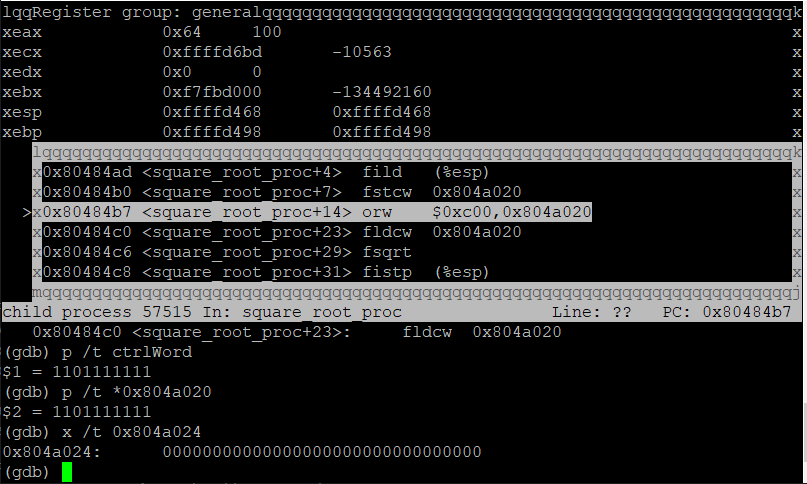
0000030 ff00 d903 002d 0000 c300

000003a











mov eax,edx

89 d0

no prefix

opcode 89: mov with op1 being a register or memory, op2 being a register

d0 binary: 1101 0000

ModR/M

mod 11: r/m is a second register

r/m 010: source operand is at the effective address of EDX,

reg 000: destination operand is the register EAX

no SIB



mov eax, [edx]

8B 02

no prefix

opcode 8B: mov with op1 being a register, op2 being a register or memory

02 binary: 0000 0010

ModR/M

mod 00: no displacement

r/m 000: destination operand is at the effective address of EAX

reg 010: source operand is the register EDX

no SIB



mov eax, [edx+8]

8B 42 08

no prefix

opcode 8B: mov with op1 being a register, op2 being a register or memory

42 08 binary: 0100 0010 0000 1000

ModR/M

mod 01: 8-bit displacement

r/m 000: destination operand is at the effective address of EAX

reg 010: source operand is the register EDX displaced by following 8 bits

no SIB

then add 0x08 to the address



mov eax, [edx+2\*ebx+8]

8B 44 5A 08

no prefix

opcode 8B: mov with op1 being a register, op2 being a register or memory

44 5A 08 binary: 0100 0100 0101 1010 0000 1000

ModR/M

mod 01: 8-bit displacement

r/m 000: destination operand is at the effective address of EAX

reg 100: source operand is ESP, which is replaced by SIB

SIB

ss: 01: index scaled by 2

index 011: index to be scaled is EBX

base 010: base register is EDX

then add 0x08 to the address