hw.md 3/23/2023

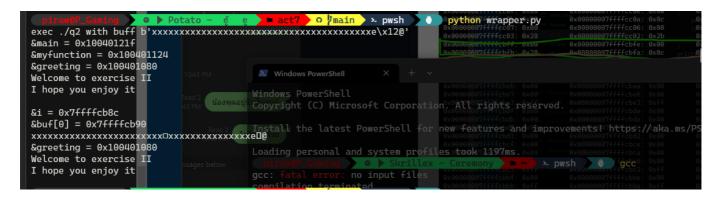
# **Activity 10: Buffer Overflow**

### **Exercise**

1. Stack Layout: Let's start with a simple program

```
\&i = 0x00000007ffffcbd0
sizeof(pointer) is 8
&buf[0] = 0x00000007ffffcba0
 0x00000007ffffcc10: 0x50
0x00000007ffffcc0f: 0x00
0x00000007ffffcc0b: 0x28
                                                                                0x00000007ffffcc0e: 0x00
0x00000007ffffcc0a: 0x0c
                                                                                                                                                               0x00000007ffffcc0d: 0x7f
0x00000007ffffcc09: 0x80
                                                                                                                                                                                                                                               0x00000007ffffcc0c: 0xff
0x00000007ffffcc08: 0x35
 0x00000007ffffcc07:
                                                                                 0x00000007ffffcc06: 0x00
                                                                                                                                                                0x00000007ffffcc05:
                                                                                                                                                                                                                 0x7f
                                                                                                                                                                                                                                                0x00000007fff
                                                                                                                                                                                                                                                                                       04: 0xff
0x00000007ffffcc03: 0x28
0x00000007ffffcbff: 0x00
                                                                                0x00000007ffffcc02: 0x2b
0x00000007ffffcbfe: 0x00
                                                                                                                                                               0x00000007ffffcc01: 0x57
0x00000007ffffcbfd: 0x7f
                                                                                                                                                                                                                                                0x00000007ffff6
                                                                                                                                                                                                                                                                                       00: 0x60
                                                                                                                                                                                                                                                                                                0xff
 0x00000007ffffcbfb:
                                                                                 0x00000007ffffcbfa:
                                                                                                                                                                0x00000007ffffcbf9:
                                                                                                                                                                                                                                                0x00000007fff
0x00000007ffffcbf7: 0x00
0x00000007ffffcbf3: 0xff
                                                                                0x00000007ffffcbf6: 0x00
0x00000007ffffcbf2: 0xff
                                                                                                                                                               0x00000007ffffcbf5: 0x00
0x00000007ffffcbf1: 0xcd
                                                                                                                                                                                                                                               0x00000007ffff
0x00000007ffff
                                                                                                                                                                                                                                                                                       f4:00x07
                                                                                                                                                                                                                                                                                       of0: 0x30
 0x00000007ffffcbef:
                                                                                 0x00000007ffffcbee:
                                                                                                                                                                0x00000007ffffcbed:
                                                                                                                                                                                                                                                0x00000007fff
0x00000007ffffcbeb:
0x00000007ffffcbe7:
                                                                                0x00000007ffffcbea: 0x00
0x00000007ffffcbe6: 0x00
                                                                                                                                                                0x00000007ffffcbe9:
0x00000007ffffcbe5:
                                                                                                                                                                                                                                               0x00000007fff
                                                  0x00
                                                                                                                                                                                                                 0x00
                                                                                                                                                                                                                                                                                       e8:00x00
                                                  0x00
                                                                                                                                                                                                                 0x00
                                                                                                                                                                                                                                                                                       e4: 0x07
 0x00000007ffffcbe3:
                                                                                 0x00000007ffffcbe2:
                                                                                                                                                                0x00000007ffffcbe1:
                                                                                                                                                                                                                                                0x00000007fff
                                                  0xff
                                                                                                                                                                                                                 0xc9
                                                                                                                                                                                                                                                                                                 0x34
0x00000007ffffcbdf:
0x00000007ffffcbdb:
                                                                                0x00000007ffffcbde: 0x00
0x00000007ffffcbda: 0x40
                                                                                                                                                                0x00000007ffffcbdd:
0x00000007ffffcbd9:
                                                                                                                                                                                                                                               0x00000007ffff
                                                  0x00
                                                                                                                                                                                                                 0x00
                                                                                                                                                                                                                                                                                       odc: 0x01
                                                                                                                                                                                                                                                                                       od8: 0xe2
                                                  0 \times 00
                                                                                                                                                                                                                 0x10
 0x00000007ffffcbd7:
                                                                                 0x00000007ffffcbd6:
                                                                                                                                                                0x00000007ffffcbd5:
                                                  0x00
                                                                                                                                                                                                                 0x00
             00007ffffcbd3: 0x00
                                                                                 AVABBBBBBB7ffffcbd2: 0x00
                                                                                                                                                                0x00000007ffffcbd1:
                                                                                                                                                                                                                 0x00
                                                                                                                                                                                                                                                0x00000007ffffcbd0: 0x00
0x00000007f+++cbc+: 0x00
                                                                                0x00000007ffffcbce: 0x00
                                                                                                                                                               0x00000007ffffcbcd: 0x00
0x00000007ffffcbc9: 0x10
                                                                                                                                                                                                                                                execution of the contract of t
0x00000007ffffcbc7: 0x00
0x00000007ffffcbc3: 0xff
0x00000007ffffcbf: 0x00
                                                                                                                                                                9x99999997++++cbc5: 0x00
0x00000007+fffcbc1: 0xcb
                                                                                                                                                                                                                                               0x000000007ffffcbc4:
0x000000007ffffcbc0:
                                                                                                                                                                                                                                                                                                0x07
0xf0
                                                                                 0x00000007ffffcbbe:
                                                                                0x00000007ffffcbba: 0xff
0x00000007ffffcbb6: 0x00
 0x00000007ffffcbbb:
                                                                                                                                                                0x00000007ffffcbb9:
 0x0000007ffffcbb7: 0x00
                                                                                                                                                                0x00000007ffffcbb5:
                                                                                                                                                                                                                                                0x00000007ffffcbb4
                                                                                                                                                                                                                 \theta \times \theta \theta
                                                                                 υχυθ000007ffffcbb2:
  0x00000007ffffcbb3: 0x00
                                                                                                                                                                                                                                                0x00000007ffffcbb0:
                                                                                                                                                                                                                                                                                                 0x36
                                                                                                                                  0x38
                                                                                                                                                                0x00000007ffffcbb1:
 0x00000007ffffcbaf:
                                                                                 0x00000007ffffcbae:
                                                                                                                                                                0x00000007ffffcbad:
                                                                                                                                                                                                                                                0x00000007ffffc
                                                                                                                                                                                                                                               0x00000007ffffcba8:
0x00000007ffffcba4:
                                                                                                                                                                0x00000007ffffcba9:
 0x00000007ffffcbab: 0x31
                                                                                0x00000007ffffcbaa: 0x30
                                                                                                                                                                                                                 0x39
0x00000007ffffcba7: 0x37
                                                                                0x00000007ffffcba6: 0x36
                                                                                                                                                                0x00000007ffffcba5: 0x35
              00007ffffcba3: 0x33
                                                                                 0x00000007ffffcba2
                                                                                                                                         o main >- pwsh > 0 gcc -o ql ql.c
```

2.



3.

hw.md 3/23/2023



### 4.

#### Ans.

I would say Yes, you can explode the buffer-overflow. However, it needs a technique so that you can bypass the canary which acts as a sentinel. There are several techniques such as canary value leak, canary value prediction, canary value overwrite, and canaray value blind overwrite.

## 5.1

## Ans.

It is not easy to exploit buffer overflow attacks, but it is not impossible either. It demands a particular amount of competence and knowledge in programming and computer security.

To exploit a buffer overflow flaw, an attacker must comprehend the target program's structure and memory management. In addition, they must be able to generate malicious input that can cause a buffer overflow and execute their own code or insert malicious payloads into the system.

Developing a software to attack buffer overflow vulnerabilities in a server can be a difficult operation, requiring an in-depth knowledge of the target system, the programming language used to construct the server, and the operating system on which it operates. In addition, it may entail advanced techniques such as shellcode injection and return-oriented programming.

## 5.2

## Ans.

By adhering to secure coding principles, it is feasible to prevent buffer overflow vulnerabilities in your code. These are some effective strategies: Stack Safety Features: Employ compiler features such as stack canaries and address space layout randomization (ASLR) to add buffer overflow protection.