Unit 5 - Week 4

Assignment 4

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-02-26, 23:59 IST.

1)
```
#include <stdio.h>

L1:  int main(void){
     L2: int l;
     L3: short s;
     L4: char c;

     L5: l = 0xdeadbeef;
     L6: s = l;
     L7: c = l;

     L8: printf("l = 0x%x (%d bits)\n", l, sizeof(l) * 8);
     L9: printf("s = 0x%x (%d bits)\n", s, sizeof(s) * 8);
     L10: printf("c = 0x%x (%d bits)\n", c, sizeof(c) * 8);
     L11: return 0;
L12: }
```

1 point

In the program given above Line ---------- and Line ---------- can cause integer overflow.
Eg: Line L1 and Line L2

- L2,L3
- L4,L5
- L6,L7
- L8.L9

No, the answer is incorrect.
Score: 0
Accepted Answers:
L6,L7

2) Which of the following statements are true?

1 point

a) The main problem in heap is the fragmentation.
b) Stack allocation is not flexible, that memory allocated cannot be changed. But heap allocation is flexible.
c) Heap allocation is done manually by the programmer.
d) The access time of heap is more that of stack.

- a
- b and c
- c and d
- All of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
All of the above

3) The contents allocated in stack are removed or deallocated when the stack frame is rolled back, where as the memory used by the heap needs to be freed either manually or by the garbage collector.

1 point

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
True

4) Match the following

1 point

1. Fast Bin	A. Double Linked List
2. Large Bin	B. Single Linked List
3. Small Bin	C. Less than 512 bytes
4. Unsorted Bin	D. Various size bins

- 1 - A, 2 - C, 3 - A, 4 - D
- 1 - B, 2 - D, 3 - C, 4 - A
- 1 - A, 2 - B, 3 - C, 4 - D
- 1 - B, 2 - A, 3 - D, 4 - C

No, the answer is incorrect.
Score: 0
Accepted Answers:
1 - B, 2 - D, 3 - C, 4 - A

5) Which of the following are the heap implementations

1 point

- dlmalloc
- jemalloc
- nedmalloc
- hoard
- All of these

No, the answer is incorrect.
Score: 0
Accepted Answers:
All of these

6) An attacker is trying to exploit format string vulnerability to find the contents of a memory location. Which of the following functions can be used by the attacker for a successful exploit?

1 point

a) vsprintf
b) vprintf
c) sprintf
d) Printf

- C and D
- A and B
- Only D
- All of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
All of the above

7) The content of the stack includes local functions, previous frame pointer, return address, followed function parameters. Of these, previous frame pointer contains the value of stack pointer address before the function call.

1 point

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
False

8) David used heap allocation techniques for memory allocation. He used statement malloc(4), to allocate memory. ---------- bytes of memory is actually allocated.

1 point

No, the answer is incorrect.
Score: 0
Accepted Answers:
(Type: Numeric) 16

9) Heap uses heap cookies or canaries to protect the return address from overwriting.

1 point

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
False

10) Xiaolu found that there is a format string vulnerability at the server, but she doesn't have access to the server code. She used some of the format specifiers like %d to determine the contents from the server, which ended up in some random values. You are advised to help Xiaolu. Which of the following is the most apt for a successful attack?

1 point

- Use %20x in the format specified to extract the contents
- Use %X%X%X%X%X%X%n format specifier to extract the contents
- Repeatedly connect to the server and try to extract the huge stack contents using a script with %x
- Use %s%s%s 3 times to get all the stack contents.

No, the answer is incorrect.
Score: 0
Accepted Answers:
Repeatedly connect to the server and try to extract the huge stack contents using a script with %x

11) To exploit Use-After-Free, we usually need to allocate a different type of the object over the one you just freed.

1 point

- True
- False

No, the answer is incorrect.
Score: 0
Accepted Answers:
True