Unit 3 - Week 2

Assignment 2

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

Due on 2020-02-12, 23:59 IST.

1) Read the following program: *0 points*

```
#include <stdio.h>

int main(){

    char a[8];
    char b[8];
    printf("%x \n",&a[7]);
    printf("%x \n",&b[-1]);
    return 0;

}
```

What will be the output of the program?

- It will not compile
- The output of both the print statements are same
- Both are not the same
- The second printf will give IndexOutOfBound error

No, the answer is incorrect.
Score: 0
Accepted Answers:
The output of both the print statements are same

2) In a Return-to-libc kind of attack which instruction needs to be inserted for a safe termination of program? *1 point*

- Exit
- Return
- Mov
- Jump

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

3) In a canary implementation which of the following operations is used to check whether the return address is corrupted or not? *1 point*

- And
- Xor
- Xnor
- Not

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

4) Assume you are using the latest Linux version. You have a code with a buffer overflow vulnerability. You exploit the vulnerability and try to overflow the buffer. You compile the code like this "gcc -g buff_overflow.c - O0" and run it. What will happen? *1 point*

- You will be successful in exploiting the vulnerability
- You will get a stack smashing error
- Your code won't compile
- You will get some unexpected behaviour in runtime

No, the answer is incorrect.
Score: 0
Accepted Answers:
You will get a stack smashing error

5) Which of the following flags you have to use to disable stack smashing? *1 point*

- f-no-stacksmasher
- f-no-canary
- f-no-stack-protector
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
f-no-stack-protector

6) If I am able to run JIT compiler, then which of the following protection is not enabled on my system? *1 point*

- W^X bit
- Canaries
- Trust Zones
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
W^X bit

7) The following program takes arg1 arg2 arg3 arg4 as arguments *1 point*

```
#include <stdio.h>
int main(int argc,char *argv[]){

    printf("%d",argc);
    printf("%s",argv[2]);
    return 0;

}
```

Arguments can be provided to gdb in the following ways

I. gdb --args ./a.out arg1 arg2 arg3 arg4
II. gdb ./a.out
(gdb) r arg1 arg2 arg3 arg4

Which of them is correct?

- I
- II
- I,II
- None of the above

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

8) To identify ROPgadgets we have to lookout for a particular instructions which end with _____ *1 point*

- 0xff
- 0x00
- 0xdeadbeef
- 0xc3

No, the answer is incorrect.
Score: 0
Accepted Answers:
0xc3

9) What is the vulnerable variables in this code? *1 point*

```
#include<stdio.h>
int myfunc_1(){
    char buff1[10];
    char buff2[5];
    scanf("%s", buf1);
    strcpy(buf1,buf2);
}

int myfunc_2() {

    char buf2[22];
    scanf("%s", buf2);
}
int main( int argc, char ** args)
{
    return myfunc_1();
    return 0;
}
```

Find the vulnerable variables

- buff1
- buff2
- buff3
- buff1,buff2
- buff1,buff2,buff3

No, the answer is incorrect.
Score: 0
Accepted Answers:
buff1

10) With both non executable stack and canaries implemented which of this attack we can prevent all forms of return oriented attacks. *1 point*

- True
- False

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