Unit 4 - Week 3

Assignment 3

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

Due on 2020-02-19, 23:59 IST.

1) If I have to change the state of ASLR in a Linux system, then which file should I look into — *1 point*

- /etc/pwd/
- /proc/sys/random_address
- /proc/sys/kernel/random
- /proc/sys/kernel/randomize_va_space

No, the answer is incorrect.
Score: 0
Accepted Answers:
/proc/sys/kernel/randomize_va_space

2) 2. Match the following: — *1 point*

Info about different states of ASLR

I. 0	i. Default
II. 1	ii. Disable
III. 2	iii. Data Segment location is not randomized

- I-i,II-ii,III-iii
- I-iii,II-ii,III-i
- I-ii,II-iii,III-i
- I-iii,II-i,III-ii

No, the answer is incorrect.
Score: 0
Accepted Answers:
I-ii,II-iii,III-i

3) Which of the following is true? — *1 point*

- Load Time Relocatable code has a very fast load time
- Code segment sharing is not an issue with Load Time Relocatable code
- Writable code segment makes a program more secure
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
None of the above

4) GOT table implementations increases the Load-time considerably, while LTR reduces runtime — *1 point*

- True
- False

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

5) Load Time Relocation of Global Data mandatorily requires a PLT as the number of functions in a library are significantly less than the number of Global Variables. — *1 point*

- True
- False

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

6) Read the following Solution and identify what problem it solves — *1 point*
Solution : Lazy binding using PLT
Problems.

- Faster run time access
- Load time relocation of global Data
- Not all functions have to be loaded to run a program, so, saves space and time
- To prevent ASLR from run-time attacks

No, the answer is incorrect.
Score: 0
Accepted Answers:
Not all functions have to be loaded to run a program, so, saves space and time

7) The heartbleed attack could have been avoided if this condition was met — *1 point*

- Data Length = Payload Length
- Data Length <= Payload Length
- Data length >= Payload length
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
Data length >= Payload length

8) I have a system with W^X, Canaries and ASLR implemented, what attack should I use to glean information: — *1 point*

- Buffer overflow
- ROP
- Return-to-libc
- Buffer Overreads

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

9) GOT corruption and Return-to-PLT are attacks that can successfully bypass ASLR — *1 point*

- True
- False

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

10) Go through the following code snippet : — *0 points*

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

        char b[]= "access_granted";
        char a[]= "User_";
        char passcode[]="User_\0access_granted";
        int len= atoi(argv[1]);

        int i=0;
        while(i<len){

            if(a[i]==passcode[i]){
            i++;
            continue;
            } else {
                printf("Doesn't match");
             return 0;
            }

        }

        printf("Passcode matched");


    }
```

Compile : gcc test2.c -o a.out
Execute it as ./a.out <length> e.g. ./a.out 5

Find the minimum value of length so that "Doesn't match" will be printed

- 5
- 10
- 13
- 15
- 22

No, the answer is incorrect.
Score: 0
Accepted Answers:
22