Consider the following binary and answer the questions below:

https://bit.ly/finalexam691

(Links to an external site.)

`In case you cannot access the shortened link for the binary, use the following google drive link (They both redirect you to the same binary)`

`https://drive.google.com/file/d/1DyceT22g0TWUaEC_PwxjvzEuNvfhRyhv/view`

`(Links to an external site.)`

1. What is the address of the function "Dumpster_Man"?

[Select] ["0x08048514", "0x0804849b", "0x080483a0", "0x080484cf"]

2. For the stack frame "Dumpster_Man", where is the canary located?

[Select] ["ebp + 20", "ebp - 14", "ebp - 20", "ebp + 14"]

3. What is the printf statement trying to print, in the function "I_Declare_Bankruptcy"?

[Select] ["If I don't have some cake soon, I might die.", "Would I rather be feared or loved? Easy. Both. I want people to be afraid of how much they love me.", "I talk a lot, so I've learned to tune myself out.", "I'm not superstitious, but I am a little stitious."]

Answer 1:

0x080484cf

Answer 2:

ebp + 14

Answer 3:

Would I rather be feared or loved? Easy. Both. I want people to be afraid of how much they love me.

Partial

Question 2

8 / 10 pts

Fill in the blanks with respect to the function "I_Declare_Bankruptcy" from the above-given binary.

```
int I_Declare_Bankruptcy(){

    int a;

     a =         [ Select ]      ["4", "20", "14", "10"]  ;

      while (        [ Select ]      ["8", "4", "2", "6"]  < a) {
          printf("..........");

          a = a -       [ Select ]     ["6", "2", "8", "4"]  ;

      }

      return       [ Select ]     ["4", "1", "5", "10"]  ;

}
```

Answer 1:

int

Answer 2:

20

Answer 3:

4

Answer 4:

2

Answer 5:

10

Question 3

12 / 15 pts

For the above binary, answer the following questions:

1. While considering the function "Dumpster_Man", what is the significance of the presence of a stack canary? Is it possible to perform a buffer overflow attack and call the function "I_Declare_Bankruptcy"? Please provide the reasoning behind your answer in 2-4 lines.

Deliverables:

Please add the following statement to your document without fail. If this statement is not present, you will lose marks.

"I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination."

exnpm (1).docx

Question 4

13 / 15 pts

Exploit the following binary to print the flag:

https://bit.ly/enpm691_final

(Links to an external site.)

`In case you cannot access the shortened link for the binary, use the following google drive link (They both redirect you to the same binary)`

`https://drive.google.com/file/d/1YXOOT2_Jn8RXfs6F3XiJ_kQbgtcFE817/view`

(Links to an external site.)

Deliverables:

Upload a document with a screenshot that satisfies the following deliverables. Additionally, please add your final payload along with steps explaining how the exploitation works.

1. Mention your name in the screenshot.
2. Show the output of date command from your VM.
3. Show the output of ifconfig command from your VM.
4. Exploitation must be outside of GDB, If you are successfully able to exploit it only from GDB, you can upload that screenshot but partial marks may be deducted.
5. **Add the following statement in your final document."I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination."**

If you are unable to exploit the binary successfully, add a screenshot with as much information as possible describing the problem that you are facing (or) the reason you suspect the exploitation is not working. (*Make sure to include the other deliverables mentioned without fail*).

ENPM691_final (1).docx

Question 5

5 / 5 pts

For the above binary, what is the flag?

A neutron walks into a bar and asks, “How much for a drink?” The bartender says, “For you? No charge."

Scissors cuts paper, paper covers rock, rock crushes lizard, lizard poisons Spock, Spock smashes scissors, scissors decapitates lizard, lizard eats paper, paper disproves Spock, Spock vaporizes rock, and as it always has, rock crushes scissors.

I'm Not Crazy. My Mother Had Me Tested.

What type of computer do you have? And Please don't say a white one..