Homework #7: Binary Exploitation

Assignment Details

This homework is due by Friday, April 2nd at **1:00 PM** ET. Remember there are no late submissions for the homework so please complete it by then.

For this assignment, be sure to document your process, don't just give the answers! Write as if you were explaining to yourself before you figured it out.

Please add the following header to your assignment:

> **Name:** {Firstname Lastname}
>
> **UID:** {Your UID}
>
> **Honor Pledge:** *I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination***.**

Assignment Goal: Apply the techniques and terminologies covered in Lecture #7 to apply basic binary exploitation concepts.

Assignment Questions

- **Question 1: (20 points, 10 points each)** Binary protections
    - Given the following binaries are you able to find which protections are enabled on them?
        1. Binary 1 (10 points)
        2. Binary 2 (10 points)

- **Question 2:** Code review

- I have a feeling this code Vanya wrote has a vulnerability! Can you find what it is?
  - Please explain what kind of vulnerability this is **(15 points)**, and how it would be exploited (show an example) **(20 points)**

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main() {
  char note[100];
  char cmd[150];

  printf("Write notes in line by line, they will be appended to './note.txt'!\n");
  while(1) {
    scanf("%99s", note);
    snprintf(cmd, sizeof(cmd), "echo %s >> ./note.txt", note);
    /* ^ This program unhackable because the input lenth is verified! */
    system(cmd);
  }
}
```

Note: To run this code, save it as note.c and run `gcc note.c -o note -w`. Then, run `./note`

- **Question 3: (35 points)** Format strings
  - This code has some data hiding the "secret"! Can you leak it anyway?

```
#include <stdio.h>

int main() {
  volatile char user_input[50];
  volatile char annoying[8] = "hahaha!";
  volatile char secret[25] = "You can't print me!"; /* Or can you? */
  char annoying2[10] = "AaAaAaAaA";

  printf("What do you want me to say? ");
  scanf("%s", user_input);

  printf(user_input);
  printf("\n");
}
```

Note: To run this code, save it as fomat.c and run `gcc format.c -o format -w -fno-stack-protector`. Then, run `./format`

Scoring

This homework will be out of 100 points total.

Point breakdown:

- Question 1
  - 10 points for first part
  - 10 points for second part
- Question 2
  - 15 points for identifying the vulnerability type
  - 20 points for a **working** demo exploit
- Question 3
  - 15 points for leaking *some* data
  - 20 points for leaking the secret
- Formatting
  - 10 points (make sure to talk through the process, not just show the answers)