**CSE 410/510 Software Security**

**Final CTF**

**March 16, 2022**

**Total 200 Points**

**Your full name:**

**Your CSE410/510 CTF platform username:**

**You are allowed to use google, or refer to lecture slides, homework, code during the exam. But, you cannot communicate with anyone in or outside of the class.**

**For each challenge, you should clearly show your exploit, screenshot of successful exploitation, and a very brief description of how you did it. Even if you fail to capture the flag, you may get some points for documenting your steps.**

**1. [40] Exploit challenge-1 to capture the flag. Source code of this challenge is NOT available. [Difficulty: medium]**

a. [4] Is this a 32-bit or 64-bit program?

b. [4] Is stack executable?

c. [4] Is there a canary to protect the stack?

b. [4] What vulnerability do you find in the program, e.g. buffer overflow, format string vulnerability

e. [4] One sentence to describe your high-level idea to capture the flag.

g. [20] screenshots, steps, and your working exploit.

**2. [40] Exploit challenge-2 to capture the flag. Source code of this challenge is available. [Difficulty: Medium]**

a. [4] Is this a 32-bit or 64-bit program?

b. [4] Is stack executable?

c. [4] Is there a canary to protect the stack?

b. [4] What vulnerability do you find in the program, e.g. buffer overflow, format string vulnerability

e. [4] One sentence to describe your high-level idea to capture the flag.

g. [20] screenshots, steps, and your working exploit.

**3. [40] Exploit challenge-3 to capture the flag. Source code of this challenge is available. [Difficulty: Easy-medium]**

a. [4] Is this a 32-bit or 64-bit program?

b. [4] Is stack executable?

c. [4] Is there a canary to protect the stack?

b. [4] What vulnerability do you find in the program, e.g. buffer overflow, format string vulnerability

e. [4] One sentence to describe your high-level idea to capture the flag.

g. [20] screenshots, steps, and your working exploit.

**4. [40] Exploit challenge-4 to capture the flag. Source code of this challenge is available. [Difficulty: medium]**

a. [4] Is this a 32-bit or 64-bit program?

b. [4] Is stack executable?

c. [4] Is there a canary to protect the stack?

b. [4] What vulnerability do you find in the program, e.g. buffer overflow, format string vulnerability

e. [4] One sentence to describe your high-level idea to capture the flag.

g. [20] screenshots, steps, and your working exploit.

**5. [40] Exploit challenge-5 to capture the flag. Source code of this challenge is NOT available. [Difficulty: Easy]**

a. [4] Is this a 32-bit or 64-bit program?

b. [4] Is stack executable?

c. [4] Is there a canary to protect the stack?

b. [4] What vulnerability do you find in the program, e.g. buffer overflow, format string vulnerability

e. [4] One sentence to describe your high-level idea to capture the flag.

g. [20] screenshots, steps, and your working exploit.