CS 3710: Intro to Cybersecurity Final Exam, summer 2023

Name

You MUST write your e-mail ID on **EACH** page. And put your name on the top of this page, too.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded. So please do that first. Sorry to have to be strict on this!

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

Plz enable me

I'm just a tiny macro

Docs wiped. Kthnxbai.

Page 2: Midterm 1 Material

1. [3 points] Is the TLS protocol, as we studied it in class, forward-secret? *Briefly*, why or why not?

2. [3 points] *Briefly,* what is a Message Authentication Code (MAC)?

3. [3 points] *Briefly* list three profitable "things" that one might engage in if one controlled a zombie botnet. (The assumption is that these things are all illegal).

4. [3 points] *Briefly* list and describe three different types of Denial of Service (DOS) attacks (but not teardrop attacks)?

Page 3: Modern Topics

5. [3 points] *Briefly* list three ways to prevent against SQL injection attacks.

6. [3 points] *Briefly,* in addition to using Tor, describe two other behaviors you would do to keep yourself anonymous online.

7. [3 points] *Briefly*, list one benefit and one drawback of each of the two types of rootkits. You can't use the same thing in reverse (so if X is larger than Y, you can't then also say that Y is smaller than X)

8. [3 points] List and *briefly* describe the four different levels of virtual machines.

Page 4: Binary Exploits

9. [3 points] *Briefly* describe three "things" you could attack with a *heap* buffer overflow.

10. [3 points] *Briefly,* what is the difference between oligomorphic, polymorphic, and metamorphic viruses?

11. [3 points] Other than the text (code) and data sections, list three other sections of a Windows Portal Executable (PE) file.

12. [3 points] *Briefly*, list the three main technical defenses against buffer overflow attacks. These are defenses from the operating system, hardware, compiler, etc. We are looking for technical defenses, not "better education" for this question.

Page 5: Miscellaneous

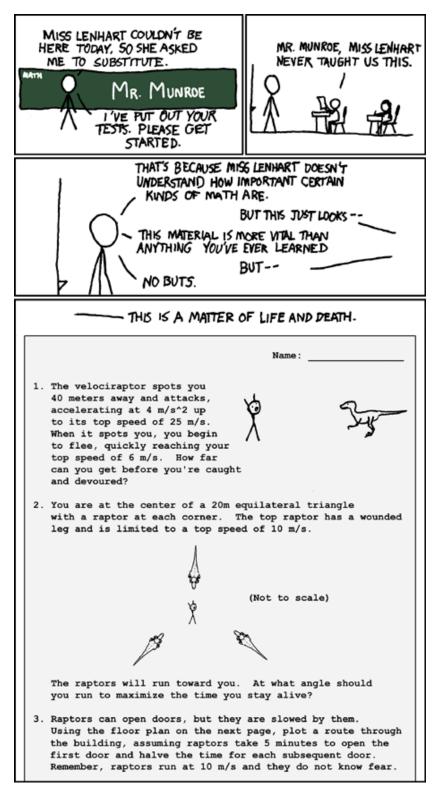
13. [3 points] *Briefly,* when can the government compel you to reveal your encrypted hard drive encryption key?

14. [3 points] *Briefly*, what is a CVE, and why do we care about them?

15. [3 points] Briefly, how does a website prevent a CSRF (Cross-Site Request Forgery) attack?

16. [3 points] Should you mine Bitcoin?

Page 6: No questions here



This page unintentionally left blank.