CS 3710: Introduction to Cybersecurity Final Exam, fall 2023

Name

Be sure to write your name and e-mail ID on top of this page.

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: First exam questions

1. [6 points] *Briefly*, list one abuse of each of the four ethical frameworks as discussed in lecture.

2. [6 points] In *bulleted list form*, list the steps of the TLS protocol. If you describe it in prose, you will not receive any credit for this question.

Page 3: Modern Topics

3. [3 points] *Briefly,* what prevents you from modifying a previous transaction in a cryptocurrency?

4. [3 points] List the two rootkit types. Choose one (either choice can get full credit) and explain why your chosen one is better than the other in some situations.

5. [3 points] List and *briefly* describe the four types of virtual machines.

6. [3 points] *Briefly* describe how Tor routes a message to a hidden service. This is meant to be a high-level overview of how it works.

Page 4: Binary Exploits

7. [3 points] *Briefly*, list three defenses that modern computers have against buffer overflow attacks. These can be compiler-based, OS-based, or hardware-based defenses.

8. [3 points] *Briefly*, Explain how a printf() format string attack works

9. [3 points] *Briefly*, list three different locations where a virus can insert its code into an executable. You can't list appending as an answer.

10. [3 points] *Briefly*, list three different code mutation techniques used by metamorphic viruses.

Page 5: xkcds

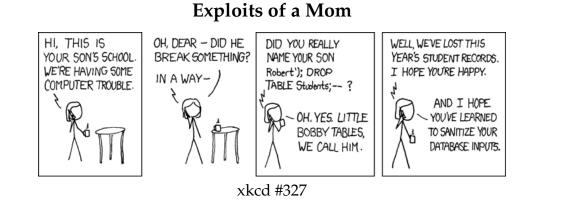
11. [3 points] On the last page of this exam are four xkcd comics. *Briefly* explain the joke for the first one ("Exploits of a Mom"), and how to defend against it.

12. [3 points] On the last page of this exam are four xkcd comics. *Briefly* explain the joke for the second one ("Security"), and what about RSA causes Cueball (the stick figure not holding the computer) to say that cracking the computer is "no good".

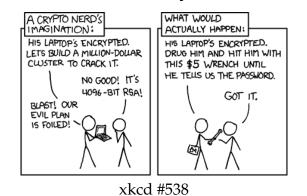
13. [3 points] On the last page of this exam are four xkcd comics. *Briefly* explain the joke for the third one ("PGP") in the context of the security mindset.

14. [3 points] On the last page of this exam are four xkcd comics. For the fourth one ("Random Number"), give the LCG (Linear Congruential Generator) formula for a more better random number generator.

Page 6: xkcd comics



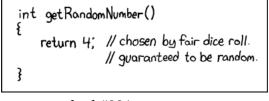
Security



PGP

How to use PGP to verify THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP
Trans worked @ Arrod in the REPLY V
BEGIN PGP SIGNED MESSAGE
Hash: SHA256
HEY,
FIRST AF ALL TELANIKE FOR TOKING CARE OF

Random Number



xkcd #221