CS 3710: Introduction to Cybersecurity Final Exam, fall 2024

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.

_____

_____

_____

_____

Phishing lines are cast,

One click, and the trap is sprung,

Wisdom shuts the door.

Page 2: First Midterm Material

1. [3 points] List the three different mathematical principles that various types of encryption are based on. Which one(s) does RSA use?

2. [3 points] For each of the layers in the TCP/IP network model, list one of the types of encryption used at that level. We are looking for a list here, not descriptions.

3. [3 points] *Briefly,* what does *forward secret* mean?

4. [3 points] *Briefly,* what is a browser fingerprint? Describe three types of information contained in such a fingerprint.

Page 3: Modern Topics, page 1

5. [3 points] List and *briefly* describe the different types of nodes in Tor.

6. [3 points] Consider a situation where your client browser has an established https connection with a web server. The web server is not in Tor, but Tor is being used to connect to that site. Assume there are n Tor nodes being used. List *all* the layers of encryption used in this situation.

7. [3 points] *Briefly,* why is cryptocurrency mining, such as that used in Bitcoin, so computationally difficult?

8. [3 points] *Briefly* describe how the "chain" part of blockchain works.

Page 4: Modern Topics, page 2

9. [3 points] List and *briefly* describe the different types of virtual machines.

10. [3 points] Given user input in a variable called `input`, write *pseudo-code* for how you would sanitize it against an SQL-injection attack. Assume that the programming language has not done anything at all to the user input (other than putting it in the `input` variable).

11. [3 points] *Briefly,* describe a *viable* use of a cross-site scripting (XSS) attack. We are looking for what one can obtain from the attack, not how to do it.

12. [3 points] *Briefly,* describe how you would defend against a cross-site request forgery (CSRF) attack, and how this defense works.

Page 5: Binary Exploits and Viruses

13. [3 points] *Briefly,* write code for virus encryption. Working assembly will get you full credit, and pseudo-code will get you partial credit.

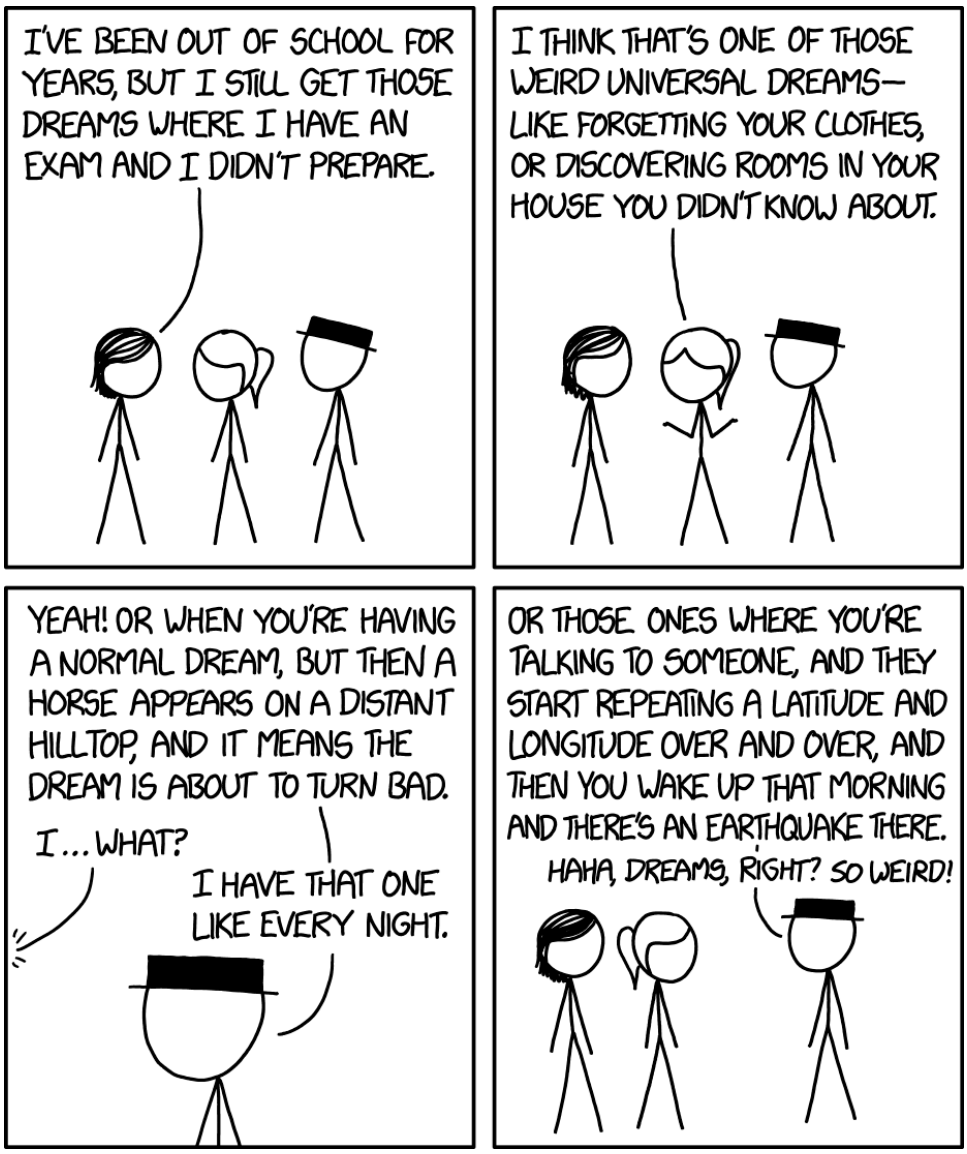
14. [3 points] *Briefly,* list three defenses against buffer overflows (other than better programming).

15. [3 points] *Briefly,* list two anti-debugging techniques that viruses use.

16. [3 points] *Briefly,* describe the difference between polymorphic, oligomorphic, and metamorphic viruses.

Page 6: No questions here

This page unintentionally left unblank.



"That's ... unsettling." "Yeah, those definitely don't sound like the normal drea- L A T I T U D E T H R E E F I V E P O I N T..."

xkcd #1943