CS 3710: Introduction to Cybersecurity Midterm 2, fall 2025

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.

_____

_____

_____

_____

Silent breach at dawn,

the gate unlatched by new code –

no patch yet exists

Page 2: SQL/XSS/CSRF and Policy

1. [3 points] Consider a web form that asks for a text value. Show an example of a SQL injection attack. You will have to make some assumptions here – just make sure that you clearly state those assumptions and that those assumptions are reasonable.

2. [3 points] *Briefly* describe a real-world example of a cross site scripting attack.

3. [3 points] *Briefly* describe how a CSRF (cross site request forgery) token could be generated – both when initially assigning it and when checking it.

4. [3 points] *Briefly,* how would SOPA and PIPA have "broken" the Internet?

Page 3: Rootkits, DOS, and Virtual Machines

5. [3 points] List and *briefly* describe the different rootkit types

6. [6 points] List and *briefly* describe the different virtual machine levels

7. [3 points] List and – if not obvious – *briefly* describe four different denial of service (DOS) attacks

Page 4: Encryption and Cryptocurrency

8. [6 points] Summarize the steps of the TLS algorithm. This can be in prose or a bulleted list. If it's easier, you can also create a network diagram (with arrows back-and-forth) such as was presented in lecture – but be sure to indicate what data is transferred for each arrow.

9. [3 points] In a cryptocurrency, how does one ensure that the hash of the block is less than the target?

10. [3 points] *Briefly,* what cryptographic operation(s) are used in a cryptocurrency?

Page 5: Stuxnet and Anonymity

11. [3 points] *Briefly,* how was Stuxnet aiming to damage its target?

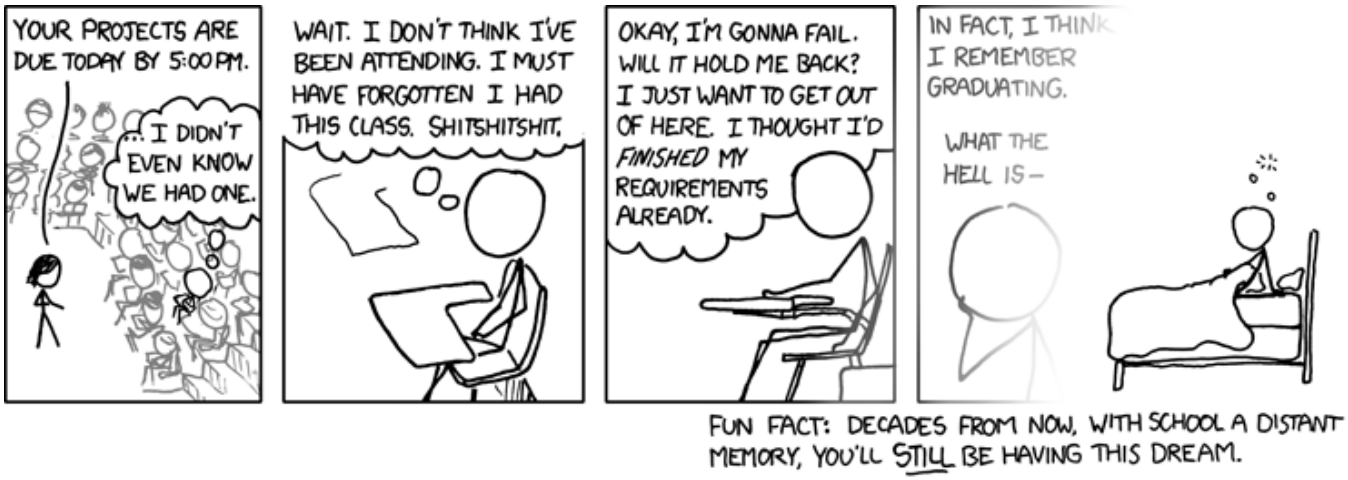
12. [3 points] Is it ethical to use Tor? If so, when? If not, why not?

13. [3 points] *Briefly* describe what happens when a Tor internal node (aka relay node) receives data. You can assume that there are no hidden services involved.

14. [3 points] Imagine a powerful (but not all-powerful) entity, such as the CIA or M6. This entity can accomplish a lot, but they do not have access to everything on the Internet. How might they track somebody who uses Tor?

Page 6: No questions here

This page unintentionally left unblank.



xkcd #2966