CS 3710: Introduction to Cybersecurity Final exam, summer 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.

Plz enable me

I'm just a tiny macro

Docs wiped. Kthnxbai.

Page 2: First midterm material & Networks

1. [3 points] *Briefly,* why is RSA so much slower than AES?

2. [3 points] *Briefly,* what is forward secrecy?

3. [3 points] *Briefly,* what is Cipher Block Chaining (CBC)? This is the same thing as encryption with Initialization Vectors (IVs). Briefly, how does it work?

4. [3 points] *Briefly,* explain how web browser cookies work.

Page 3: Binary Exploits

5. [3 points] List 4 different ways that viruses encrypt themselves. We are looking for the specific operations here.

6. [3 points] *Briefly*, what are the differences between the three virus encryption types: oligomorphic, polymorphic, and metamorphic.

7. [3 points] List three defenses against buffer overflows provided by the OS and/or compiler. This is for C/C++, not interpreted languages.

8. [3 points] What is the best way to prevent against `printf()` format string attacks?

Page 4: Modern topics

9. [3 points] *Briefly,*, what prevents one from changing a past transaction in a cryptocurrency to make themselves rich?

10. [3 points] *Briefly,* if one were to create a compromised node in the Tor network, what information would you be able to ascertain? You can be an entry node, exit node, or internal node. This is not a hidden service, though.

11. [3 points] *Briefly,* describe the rootkits used in Stuxnet.

12. [3 points] List a viable use of a cross-site scripting attack.

Page 5: Miscellaneous

13. [3 points] *Briefly,* describe one of the forensics case studies we discussed in lecture.

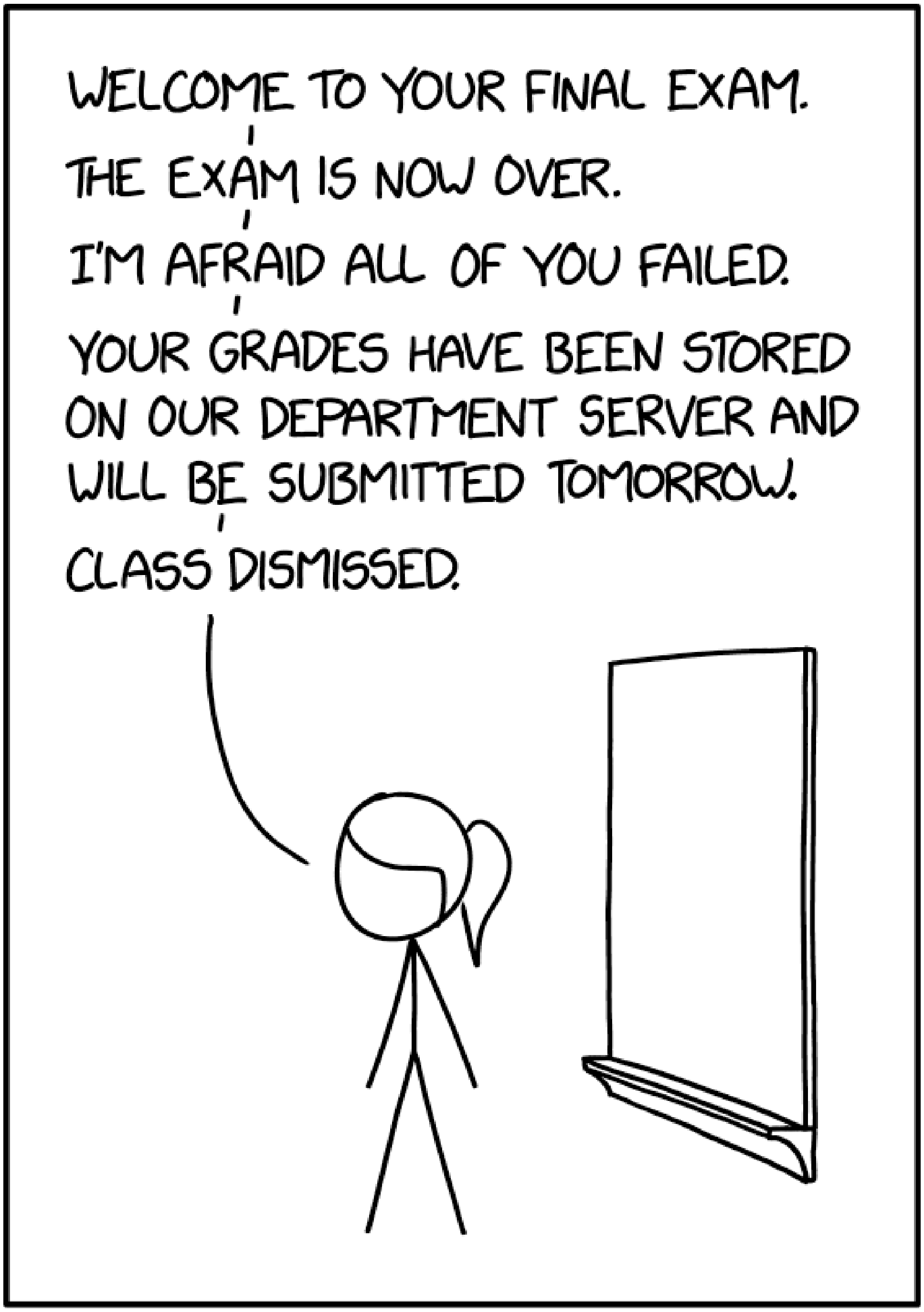
14. [3 points] List six different sections of an executable file. If you don't remember the correct name, you can give a *brief* description of the section instead.

15. [3 points] List four levels of virtual machines. If you don't remember the correct name, you can give a *brief* description of it instead.

16. [3 points] I strive to present the information in this course in a politically neutral way. To see if I succeeded in doing so, please write what you think my political views are. If nobody gets it right, or everybody has different answers, then I know I succeeded. You will get full credit as long as you write what you think – I won't grade for content. If you don't know, or can't tell, that's a valid answer as well.

Page 6: No questions here

This page unintentionally left unblank.


WELCOME TO YOUR FINAL EXAM.
THE EXAM IS NOW OVER.
I'M AFRAID ALL OF YOU FAILED.
YOUR GRADES HAVE BEEN STORED ON OUR DEPARTMENT SERVER AND WILL BE SUBMITTED TOMORROW.
CLASS DISMISSED.

CYBERSECURITY FINAL EXAMS

xkcd #2385