CS336 Homework #5

Due: Friday, May 12, 2023, 5:00 pm
Points: 120 pts

1. (20 points) Investigate the details of the **integer overflow attack**, how it works, and how the attack string it uses is designed. Then experiment with implementing this attack (**write a piece of code yourself** which has integer overflow vulnerability, take a screenshot of running it and show me that you have successfully exploited an integer overflow vulnerability).

2. (20 points) Investigate the details of the **buffer overflow attack**, how it works. Then experiment with implementing this attack against a suitably vulnerable test program (**write a piece of code yourself** which has buffer overflow vulnerability, take a screenshot of running it and show me that you have successfully exploited a buffer overflow vulnerability).

3. (10 points) Explain why genetic diversity is a good principle for secure development. Cite an example of lack of diversity that has had a negative impact on security.

4. (10 points) What is incomplete mediation? What are the potential problems with incomplete mediation? What can we do for better checking user input?

5. (10 points) List three controls that could be applied to detect or prevent off-by-one errors.

6. (10 points) Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

7. (10 points) Suppose that while trying to access a collection of short videos on some website, you see a pop-up window stating that you need to install this custom code in order to view the videos. What threat might this pose to your computer system if you approve this installation request?

8. (10 points) Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client, web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?

9. (5 pts) What is clickjacking attack? Suggest a technique by which a browser could detect and block clickjacking attacks?

10. (5 pts) Explain why spam senders frequently change from one email address and one domain to another. Explain why changing the address does not prevent their victims from responding to their messages.

11. (10 pts) Why does a web server need to know the address, browser type, and cookies for a requesting client?