United International University

Department of Computer Science and Engineering

Final Exam, Spring 2025

CSE 4531: Computer Security

Total Marks: 40, Duration: 2 Hours

Any examinee found adopting unfair means will be expelled from the trimester/program as per UIU disciplinary rules.

Answer all the questions.

1.	a) Suppose you have received a digitally signed message that claims to have been signed by Alice and that you want to verify this signature. Discuss why you need a Certification Authority here.	**3**
	b) What are zero-day exploits and how to prevent them? Give an example of such an attack.	**3**
	c) Suppose you just got a call from the University System Administrator, who says that he has checked the network configurations and traffic and finds that you are flooding the varsity BSCSE results website with excessive requests to overload the system so that other students cannot access the portal and resources. (i) **Which attack** are you supposed to conduct? However, you know you are not doing this, rather, someone is using your network credentials, such as IP or MAC address. (ii) **In this case, which attack** are you facing? (iii) Among interruption, interception, modification, and fabrication, in **which categories** do these two attacks lie? In each part, justify your answer with short explanations.	**4**
2.	a) A banking system suddenly experiences fraudulent transactions after an employee in the software division is fired. What kind of malware could be responsible for such activities, and what are the countermeasures to prevent them?	**3**
	b) Explain buffer overflow attacks with an example. How to protect such attacks?	**3**
	c) How is a botnet used to launch DDoS attacks? Explain with a figure.	**4**
3.	a) Assume a web server that has a database table that contains user login credential stored without any encryption or hashing techniques. The website also has a form that is vulnerable to **SQL Injection attacks**. Explain potential exploitation of the website and design a SQL Injection attack that can retrieve the users' username and passwords. Assume the names of the database tables and columns as needed.	**3**

	b) An attacker crafts a malicious web page that contains a hidden form which, when visited by a logged-in user of the e-commerce site, automatically submits a request to change the user's email address to the attacker's address. The victim, while logged into their e-commerce account, clicks a link on a social media post and unknowingly loads the malicious web page. As a result, their registered email is silently updated to the attacker's email. Briefly describe what kind of attack is occured here and what steps could have been implemented to stop it?	**3**
	c) Employees within a large corporation report unauthorized access to their accounts. Security investigations reveal that an attacker within the internal network is manipulating the Address Resolution Protocol to redirect network traffic to a malicious server under their control. Explain how this attack enables the attacker to steal employee credentials. Then, describe some security measures that can be implemented to prevent and mitigate this type of attack.	**4**
4.	a) Calculate the following big moduli: $7^{927} \; mod \; 13$	**2**
	b) Compare symmetric and asymmetric cryptography with example.	**4**
	c) Charlie wants to use RSA for secure communication. He chooses two prime numbers, p=11 and q=17, and selects e=9 as the public exponent. Determine the private key (d). Then, encrypt the message m=4 with the public key to compute the ciphertext. And verify that decryption retrieves the original message.	**4**