United International **University**

Department of Computer Science and Engineering

Final Exam, Fall 2024

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) How is botnet used to launch DDoS attacks? Explain with a figure.	**3**
	b) If a system uses 32-bit salt for each user ID and its user picks a password from a 100,000 word dictionary, then what is the total search space for attacking the salted password? Show necessary calculations.	**3**
	c) What is stack smashing attack? How to launch a buffer overflow attack using an unsafe library function? Explain with necessary example.	**4**
2.	a) A ransomware attack locks all medical records, thereby preventing doctors from accessing patient data during an emergency. Which part of the CIA Triad is violated? Suggest methods to defend against such attacks.	**3**
	b) Kim's computer is behaving strangely—firewall settings are changing automatically, and security logs are being erased. When he scans for malware, the scan results show no issues. What type of malware could be responsible for this? Why is this particular malware difficult to detect?	**3**
	c) What would be the financial advantage for a virus developer to create lots of different malicious code instances that all exploit the same vulnerability yet have different malware signatures? What type of virus is it? How to make such a virus?	**4**
3.	a) What is SYN flooding attack? What is its impact on a web server? Explain with a figure.	**3**
	b) Explain cross-site scripting attack to a web server. How can you prevent such an attack?	**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) List three main requirements of a cryptographic hash function. Give examples of such hash functions.	**3**
	b) How can an attacker launch a man-in-the-middle attack on Diffie-Hellman key exchange protocol? Explain with a necessary figure.	**3**
	c) Charlie wants to use RSA for secure communication. He chooses two prime numbers p=7 and q=23, and selects e=13 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**