Course: IT 221 Information Assurance and Security
MIDTERM Exam
462 - Date: 12/03/2025 Duration: *1 hour*

Student Name: **Student ID:** **S.N:**

For Instructor use only

CLOs	k1	k2	k3	S1	S2	S3	S4	V1	V2
Question number	3+4				2				
Allocated mark	10				5				
Earned mark									

Total Mark
/20

The exam starts here

Question 1 **(___/5 pts)**

Decide if the following statements are True or False; Correct the False ones if any.

1. Security patch includes enhancements to the software to provide new or expanded functionality	
2. UEFI is a firmware used on early computers to hold the boot process	
3. Encryption is changing original text into a secret message using cryptography	
4. Stream cipher - takes one character and replaces it with another	
5. The diffusion principle in cryptography means that the key does not relate in a simple way to the ciphertext	
6. Rootkit is a computer code that lies dormant until it is triggered by a specific logical event	
7. Macro virus is a series of instructions that can be grouped together as a single command, it is a common virus that infects data files	
8. When backdoors installed on a computer, they allow the attacker to return later and bypass security settings	
9. The hacktivists are attackers who may be directed at targets such as the military installations, power plants, air traffic control centers, and water systems	
10. A single defense mechanism layer is enough to defend against various types of malwares	

Question 2 **(___/5 pts)**

Choose the suitable answer:

1. Flaw or weakness that allows a threat agent to bypass security:
   a. Vulnerability
   b. Risk
   c. Threat
   d. Attack
2. Trusted OS hardening technique includes:
   a. Read-only file system
   b. Least privilege
   c. Kernel pruning
   d. All above true

3. _____ is a drive encryption software that is included in Microsoft Windows.
   a. BitLocker
   b. Pretty Good Privacy (PGP)
   c. GNU Privacy Guard (GNUPG)
   d. Trusted platform module (TPM)
4. An infected computer that is under the remote control of an attacker:
   a. Bot
   b. Zombie
   c. a and b
   d. Trojan
5. Attacker pretends to be someone else:
   a. Phishing
   b. Impersonation
   c. Spamming
   d. Hoaxes
6. An electronic variation of dumpster diving is to use Google's search engine to look for documents and data posted online
   a. Google surfing
   b. Google indexing
   c. Google Dorking
   d. Google diving
7. Takes as input a string of any length and returns a string of any requested variable length:
   a. Stream cipher
   b. Block cipher
   c. Spong function cipher
   d. Hashing
8. Distributing and maintaining a secure single key among multiple users distributed geographically is a weakness of:
   a. Public key cryptography
   b. Private key cryptography
   c. Digital signatures
   d. Hashing
9. OS in firmware that is designed to manage a specific device like a digital video recorder or video game console:
   a. Kiosk OS
   b. Server OS
   c. Appliance OS
   d. Network OS
10. Barriers, guards and motion detection devices are used for:
    a. Operating System Security
    b. External Perimeter Defenses
    c. Internal Perimeter Defenses
    d. Computer device security

Question 3 (5 pts) Answer the following questions:

a. **Define Phishing and give Two variations of phishing attacks?** **(__/ 3 pts)**

b. Mention Two of Secure **DevOps methodology** practices: **(__/ 2 pts)**

Question 4 (5 pts)

a. Using ROT13 Cryptographic algorithm, encrypt the following text: **(__/2 pts)**

Plaintext	R	a	m	a	d	a	n	M	u	b	a	r	a	k
Ciphertext														

What is Supply chain infections? Why it is considered dangerous? **(__/3 pts)**

Best wishes….