Roll No. _____ Name _____ Group _____

PIS105: Secure Coding **20 Feb 2025** **Time: 20 Minutes** **MM:10**
Faculty: Dr. Lokendra Vishwakarma

Thapar Institute of Engineering & Technology
Computer Science & Engineering Department
QUIZ-1 (SET-A)

Instructions: 1. Assume missing data, if any, suitably. **2.** Write the correct option in the box ONLY. Answers not marked in the boxes, will not be evaluated. **3.** Overwritten answers will not be entertained. **4.** In case you think no option is correct, write option E.

1	2	3	4	5	6	7	8	9	10	11	12	13
C	A	B	C	C	B	C	D	C	D	ABC	ABC	B

1. **Which of the following is *NOT* a part of the CIA triad?** [0.5]
A. Confidentiality B. Integrity C. Authentication D. Availability

2. **What is the primary difference between a virus and a worm?** [0.5]
A. A virus requires a host program, while a worm spreads independently.
B. A worm requires a host program, while a virus spreads independently.
C. A virus always encrypts data, while a worm does not.
D. A worm is only transmitted via email attachments.

3. **In cryptanalysis, which attack assumes the attacker has access only to the ciphertext?** [0.5]
A. Known plaintext attack B. Ciphertext-only attack
C. Chosen ciphertext attack D. Chosen plaintext attack

4. **Which of the following is an example of a passive attack?** [0.5]
A. SQL Injection B. Man-in-the-Middle attack C. Eavesdropping D. Ransomware attack

5. **What is the primary goal of a Denial-of-Service (DoS) attack?** [0.5]
A. To steal confidential information B. To alter the integrity of a system
C. To make a service unavailable to legitimate users D. To inject malware into the system

6. **What is the key principle behind "Secure by Default" in SD3?** [0.5]
A. Default settings should prioritize performance over security
B. Security features should be enabled by default
C. Encryption should always be manually activated by the user
D. None of the above

7. **A security threat is categorized as Tempering and Elevation of Privilege in which threat model framework?** [0.5]
A. DREAD B. Attack Tree C. STRIDE D. All of Them

8. **Which of the following is the possible attack if the developer lacks boundary checking when writing to the memory?** [0.5]
A. Invalided Input B. Race Condition C. Weakness in Authentication D. Heap Overflow

9. **Which attack exploits the delay between checking and using a resource in race conditions?** [0.5]
A. Buffer Overflow B. SQL Injection
C. Time-of-Check to Time-of-Use (TOCTOU) D. cryptographic practices

10. **In the DREAD model, which factor assesses how easily an attacker finds the vulnerability?** [0.5]

A. Damage Potential B. Reproducibility C. Exploitability D. Discoverability

---

11. **What happens when the following C program is executed with a long string input?** [**Note:** Select multiple option if other options are correct.] [2]

```
#include <stdio.h>
#include <string.h>

void vulnerableFunction(char *input) {
    char buffer[10];
    strcpy(buffer, input);
    printf("Input received: %s\n", buffer);
}

int main() {
    char userInput[100];
    printf("Enter input: ");
    scanf("%s", userInput);
    vulnerableFunction(userInput);
    printf("This line may not print!\n");
    return 0;
}
```

A. Buffer overflows and corrupts adjacent memory.
B. Overwrites the return address, causing a segmentation fault (crash).
C. "This line may not print!" might not be executed due to stack corruption.
D. None of the Above

---

12. **What will happen if an attacker enters %x %x %x %x in the following vulnerable program?** [**Note:** Select multiple option if other options are correct.] [2]

```
#include <stdio.h>

int main() {
    char userInput[50];
    printf("Enter input: ");
    scanf("%s", userInput);
    printf(userInput);  // Vulnerable line
    return 0;
}
```

A. %x %x %x %x will read stack memory values.
B. Potential arbitrary code execution
C. `printf("%s", userInput);` fix the issue.
D. None of the Above

---

13. **A company is comparing DDoS Attack vs. Phishing Attack based on the DREAD model:**

Attack	D	R	E	A	D
DDoS Attack	8	7	6	9	10
Phishing Attack	7	10	10	8	9

Calculate DREAD score and find which attack is more severe. [1]

A. DDoS B. Phishing C. Both are Equal D. Both are at Medium Risk level

---