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-B)

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
D	B	A	B	C	C	C	B	C	D	C	ABC	A

1. **Which of the following is a part of the CIA triad?** [0.5]

A. Access Control B. Impersonation C. Authentication D. Availability

2. **What is the key difference between a penetration test and a vulnerability assessment?** [0.5]

A. A penetration test only identifies vulnerabilities, whereas a vulnerability assessment actively exploits them.
B. A penetration test actively exploits vulnerabilities, whereas a vulnerability assessment only identifies them.
C. Penetration Testing and Vulnerability assessment are both the same thing.
D. A penetration test is automated process, while a vulnerability assessment is manual process.

3. **In cryptanalysis, which attack assumes the attacker has access to the random pair of plaintexts and ciphertexts?** [0.5]

A. Known plaintext attack B. Ciphertext-only attack
C. Chosen ciphertext attack D. Chosen plaintext attack

4. **Which of the following is a category of a passive attack?** [0.5]

A. Replay B. Release of message contents
C. Masquerade D. Denial of Service

5. **What is the primary goal of a Interruption 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. **Choose the correct option for the below statements.**
I. A security risk is classified as **vulnerability** if it is recognized as a possible means of attack.
II. A security risk with one or more known instances of a working or fully implemented attack is classified as an **exploit**. [0.5]

A. Only I is TRUE B. Only II is TRUE C. Both are TRUE D. Both are FALSE

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. **In Secure Software Development Life Cycle (SSDLC), at which stage should threat modeling ideally be performed?** [0.5]

A. During deployment B. During design and requirement analysis
C. After a security breach D. During maintenance

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 STRIDE framework, the role based access control is mitigation strategy for which threat?** [0.5]

A. Tampering B. Information Disclosure C. Denial of Service D. Elevation of Privilege

---

11. **A threat model (Attack Tree) for an IoT system has the following attack probabilities:** [2]

Attack PATH	**Step-1**	**Step-2**	**Step-3**	**Total Probability**
$Path_A$	30%	40%	50%	?
$Path_B$	60%	20%	80%	?
$Path_C$	50%	50%	50%	?

Calculate total attack probability of each attack and find which attack path posses the highest risk?

A. $Path_A$ B. $Path_B$ C. $Path_C$ D. All have same probability

---

12. **What will happen if an attacker enters %x %x %x %x in the following vulnerable program?** [**Note:** Select multiple option if more than one 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 security analyst evaluates four cybersecurity threats using the DREAD model:**

Attacks	D	R	E	A	D
A1	8	10	9	7	9
A2	9	8	9	10	10
A3	7	9	10	5	10
A4	6	7	8	7	9

Calculate DREAD score and Rank the threats from highest to lowest risk. [1]

A. A2 A1 A3 A4 B. A1 A2 A3 A4 C. A4 A3 A2 A1 D. A3 A4 A2 A1
