Graphic Era HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

Mid Term (Odd) Semester Examination October 2024

Roll no...2294038.....

Name of the Course and semester: B.Tech Vth Semester
Name of the Paper: Computer System Security
Paper Code: TCS-591
Time: 1.5 hour

Maximum Marks: 50

Note:

(i) Answer all the questions by choosing any one of the sub questions
(ii) Each question carries 10 marks.

Q1. (10 Marks)

a. Provide a comprehensive definition of fuzzing within the context of computer system security. Differentiate between the following fuzzing techniques:
i) Black-box fuzzing
ii) White-box fuzzing
iii) Grey-box fuzzing

OR

b. What is sandboxing, and how does it help mitigate the risks associated with untrusted code execution? What challenges do developers face in implementing effective sandbox environments?"

Q2. (10 Marks)

a. What is a buffer overflow attack, and how does it exploit vulnerabilities in software systems? Provide a case study to illustrate the mechanisms and impact of such an attack.

OR

b. What is the Dirty COW attack, and how does it occur within software systems? Explain the underlying mechanisms that enable this vulnerability and how it leads to privilege escalation.

Q3. (10 Marks)

a. What are cybersecurity vulnerabilities formed in software systems, and what are the different types of vulnerabilities that can be exploited by attackers?

OR

b. What is access control in computer system security? How does the Zero Trust security model influence the design and implementation of access control mechanisms

Q4. (10 Marks)

a. What are the most common types of cyber-attacks targeting computer systems? what training and awareness programs can organizations implement to counteract these threats?

OR

b. What is a web security model, and what are the key components that contribute to securing web applications against potential threats and vulnerabilities?

Q5. (10 Marks)

a. What is a race condition? Consider a banking application where two transactions are processed simultaneously. Explain how a race condition could result in an incorrect balance and what security measures could be implemented to prevent this.

OR

b. What is the difference between static and dynamic analysis tools in software security? Discuss the role of these tools in identifying vulnerabilities and improving software robustness.