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

End Term (Odd) Semester Examination November 2025

Roll no.....

Name of the Course and semester: B.Tech CSE V CYBER
Name of the Paper: Computer System Security
Paper Code: TCS 597

Time: 3 hour Maximum Marks: 100

Note:

(i) All the questions are compulsory.
(ii) Answer any two sub questions from a, b and c in each main question.
(iii) Total marks for each question is 20 (twenty).
(iv) Each sub-question carries 10 marks.

Q1. (2X10=20 Marks)
a. Compare static, dynamic program analysis techniques for vulnerability detection with suitable case studies. CO1
b. Analyze privilege escalation techniques used in modern OS exploitation and justify why privilege isolation is critical. CO2
c. Design a secure memory handling code snippet in C to prevent buffer overflow and format string attacks. CO2
Q2. (2X10=20 Marks)
a. Apply a format string vulnerability in a printf(user_input) call to leak stack memory addresses. Demonstrate with code. CO2
b. Evaluate the security impact of the Shellshock vulnerability in a web server using CGI scripts. Propose a mitigation beyond patching. CO2
c. Given a web application that processes both server-side and client-side user inputs, differentiate between Stored, Reflected, and DOM-based XSS attacks in terms of their injection vectors, payload execution context, and persistence mechanisms. Illustrate with appropriate examples or attack scenarios. CO2
Q3. (2X10=20 Marks)
a. Create a TLS-enabled web client-server communication script. CO3
b. Implement a simple keylogger detection mechanism using Android's accessibility service monitoring. CO4
c. Analyze why spyware persists across reboots and evaluate hardware-backed keystore as a countermeasure. CO3
Q4. (2X10=20 Marks)
a. Apply a race condition exploit between access() and open() in a file access program. CO4
b. Analyze Rootkit behavior and smartphone attack methods. CO3
c. Compare Android and iOS app security models. CO3
Q5. (2X10=20 Marks)
a. Examine the architectural flaws in speculative execution that give rise to Spectre and Meltdown attacks. Model the data flow path exploited during transient execution and propose a hardware-level

countermeasure design that mitigates these vulnerabilities without significantly degrading performa	CO5
b. Analyze the security implications of supply chain attacks in SCADA systems.	CO5
c. Develop a simple access control mechanism using Linux capabilities to restrict a program's privileges	CO5 CO6