PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004

Department of Applied Mathematics and Computational Sciences

M. Sc Cybersecurity & V

CONTINUOUS ASSESSMENT TEST 2 Date: 29-10-2025

23XC54 - Software Security and Exploitation

Time: 1 Hour 30 min. **Maximum Marks: 40**

INSTRUCTIONS:

1. Answer **ALL** questions. Each question carries 20 Marks.
2. Subdivisions (a)(i) and (a)(ii) carries 2 marks each, subdivision (b) carries 6 marks each and subdivision (c) carries 10 marks each.
3. Subdivisions (a) and (b) will be with no choice and Subdivision (c) may be with choice but not in more than 1 question.
4. Course Outcome Table:

Qn.1	CO. 3	Qn.2	CO. 4

1. a) i) What is meant by shared kernel and process address space? How is it implemented? ***[BTL:1]***

   ii) How ret2usr attack is performed? ***[BTL:1]***

   b) What is the vulnerability present in the below program? Explain *it in detail using the* below code. ***[BTL:2]***

```
1 void win32k_entry_point(...) {
2   ...
3   my_struct = (PMY_STRUCT) lParam;
4   if (my_struct ->lpData) {
5     cbCapture = sizeof(MY_STRUCT) + my_struct->cbData; //1st fetch
6     ...
7     my_allocation = UserAllocPoolWithQuota(cbCapture, TAG_SMS_CAPTURE))
8     if ( my_allocation != NULL) {
9       RtlCopyMemory(my_allocation, my_struct->lpData, my_struct->cbData); //2nd fetch
10    }
11  }
12  ...
13 }
```

   c) Answer the following questions. **[BTL:3]**

   - What is dynamic tracing in Linux? Depict the framework for dynamic tracing. How kprobes is used for dynamic tracing? (5 marks)

   - Explain the kernel exploit mitigation mechanisms - KPTI and KASLR. What kind of kernel exploits are mitigated by these mechanisms? Mention their effectiveness in mitigating kernel exploits and their limitations. (5 marks)

2. a) i) What is a seccomp in Linux? How can it be enabled? **[BTL:1]**

   ii) Write about SMEP vs SMAP. **[BTL:1]**

   b) Explain in detail the Linux kernel architecture and the process and memory subsytems of the kernel. **[BTL:2]**

   c) How Dirty COW exploit works in Linux? Write code and explain. **[BTL:3]**