PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004

Department of Applied Mathematics and Computational Sciences

M. Sc Cyber Security & V Semester

CONTINUOUS ASSESSMENT TEST 1 Date: 28-08-2025

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. 1	Qn.2	CO. 2

1. a) i) What is memory safety? When is a program said to be memory unsafe? Is C language memory safe? Why? **[BTL:1]**

ii) Consider the C program given below. Construct a payload to perform stack overflow exploit using the given 30 byte shellcode. Explain each part of the payload and justify its need and size. Draw the stack layout **before and after** the execution of strcpy() function. Which protection mechanism(s) can prevent this particular exploit? Justify the same.

```
#include<stdio.h>
#include<string.h>
int main(int argc,char *argv[])
{
  char str[64] = "hai";
  char buffer[64];
  strcpy(buffer,argv[1]);
}
```

Shellcode:

```
\x48\x31\xd2\x52\x48\xb8\x2f\x62\x69\x6e\x2f\x2f\x73\x68\x50\x48\x89\xe7\x52\x57\x4
8\x89\xe6\x48\x31\xc0\xb0\x3b\x0f\x05
```

[BTL:1]

b) What is the basic idea behind ASLR? Do you think ASLR is a very effective protection mechanism? Why or why not? What is PIE? How does it support ASLR? **[BTL: 2]**

c) **[BTL: 3]**

Return-to-libc (ret2libc) attacks are a type of exploit that takes advantage of vulnerabilities in software to execute malicious code. Explain.

- The role of the libc library in ret2libc attacks
- How attackers use the return-to-libc technique to bypass DEP and ASLR

Provide specific example of ret2libc attacks and discuss the challenges and limitations of this type of attack. Additionally, discuss potential mitigation strategies that can be used to prevent or detect ret2libc attacks.

2. a) i) What is the primary cause of a format string vulnerability in C? **[BTL:1]**
ii) Consider the StackGuard (Stack Canary) system to prevent "Buffer Overflows". Where on the stack the canary should be placed, at what points in the code the canary should be written, and at what points it should be checked, to prevent buffer overflow exploits that take control of the return address? **[BTL:1]**

[BTL:2]

b)
Explain the process (as steps) of how a library function is dynamically linked at run time. For example, if a program is calling printf function which is dynamically loaded from the libc.so library, how is printf's code loaded into memory when it is actually invoked. Brief about the data structures involved..

[BTL:3]

c)
Describe the key concepts and ***steps involved in a ROP attack***, including:

- The role of gadgets in ROP attacks
- ROP chaining
- The importance of stack alignment and gadget selection
- How ROP attacks can be used to bypass common exploit mitigation techniques, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR)