Semester	**Fall Semester 2024-2025**
Course Detail	**BCSE321P - Malware Analysis**
Class No	**VL2024250102147**
Slot	**L23+L24**
Time	**11:40 to 1:20PM**
Date	**21-11-2024**

Marks Distribution:

S.NO	COMPONENTS	MARKS
1.	Web Analysis (20 Marks)	
2.	Tool Analysis (20 Marks)	
3.	VIVA (10 Marks)	
4.		
5.		
	Total (50)	

Submission Requirements

a) Detailed explanations for each identified threat indicator
b) Screenshots of relevant findings
c) Write the Question 1.1 on Answersheet

Question : 1 - ANYRUN

1) Initial File Analysis
    a) Document the file metadata (name, size, hash values)
    b) Select Windows 10 (x64) as the analysis environment
    c) Set appropriate network connection parameters
2) Interactive Analysis
    a) Monitor and document real-time process creation
    b) Identify and record any network connections established
    c) Document registry modifications
3) Process Tree Analysis
    a) Generate and interpret the process behavior graph
    b) Identify parent-child process relationships
    c) Document any process injection attempts
    d) Highlight suspicious process names or behaviors
4) Network Analysis
    a) Analyze HTTP(s) requests and response
    b) Document all external IP connections
    c) Record any DNS queries made by the malware
5) Report Generation
    a) Create a comprehensive HTML report including
    b) Process behavior graphs
    c) Network activity summary
    d) System modifications
    e) Screenshots of key events

Question : 2 – IDAPRO

1) IDA Pro and identify:

a) File format and architecture
b) Entry point address
c) Compiler used
d) Import table contents

2) Main function:
a) Identify the function prologue
b) Locate and rename important functions
c) Document any string references

3) Analyze the program's control flow:
a) Create a flowchart of the main function
b) Identify and document all conditional branches
c) List any loops present in the code

4) Examine cross-references:
a) Find all references to the string "Password:"
b) Document functions calling the main function
c) List external API calls

5) Data analysis tasks:
a) Locate and document any encrypted strings
b) Identify global variables
c) Document any interesting data structures
d) Document the program's basic functionality
e) Identify potential security checks

6) Export and document:
a) Generate an exports table
b) Save your renamed functions
c) Create function comments for key procedures
d) List suspicious API calls
e) Document any network-related functions
f) Identify file system operations