17700

BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2024
Course Name – Malware Analysis and Reverse Engineering
Course Code - MNC27202A (T)
(Semester II)

Full Marks : 40 **Time : 2:0 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 10=10

1. *Choose the correct alternative from the following :*

(i) Which of the following are possible signs of a malware infection?
   a) Slow system performance
   b) Erratic Computer Behavior
   c) Slow internet connection
   d) all of these

(ii) Name Which of the following statements is true about the Trojans.
   a) Trojans perform tasks for which they are designed or programmed
   b) Trojans replicates them self's or clone them self's through an infections
   c) Trojans do nothing harmful to the user's computer systems
   d) None of these

(iii) What is the work of decompilers?
   a) Converting binary code into native code
   b) Converting native code into binary code
   c) a and b
   d) None of these

(iv) Define the intended use case of Joebox related to threat detection.
   a) URL analysis
   b) Phishing Detection
   c) a and b
   d) None of these

(v) Identify a remote access trojan.
   a) Conficker
   b) Worm
   c) a and b
   d) None of these

(vi) Which of the following methods is NOT commonly used for memory dumping.
   a) Physical Memory Dump
   b) Hybrid Dump
   c) File System Backup
   d) Process Memory Dump

(vii) In memory forensics, what is the main focus of analyzing processes in memory dumps?

a) To identify installed software
b) To determine the hardware configuration
c) To uncover evidence of malicious activity
d) To retrieve deleted files

(viii) Select the primary use of x64dbg in cybersecurity from the following.

a) Software development
b) Malware analysis and reverse engineering
c) Network configuration
d) Database management

(ix) Select the correct statement about DLL export enumeration.

a) It is used to compile a DLL into an executable.
b) It identifies all functions and symbols exported by a DLL.
c) It encrypts the functions within a DLL.
d) It removes unnecessary functions from a DLL.

(x) What should you choose to analyze if you suspect a process has been compromised by shellcode injection?

a) Network logs
b) Process memory regions
c) Firewall rules
d) Disk usage logs

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the concept of "Static Analysis" in malware analysis and its advantages and limitations. (3)
3. Summarize the capabilities of The Sleuth Kit. (3)
4. Describe JIT debugger and its common usage. (3)
5. Define a "watchpoint" in the context of debugging. (3)
6. Explain the process of code injection. (3)

OR

Explain YARA and its role in pattern matching for identifying malware and other malicious files. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Explain the concept of breakpoints in debugging and how they are used to control program execution. (5)
8. Describe the stages of Reverse Engineering. (5)
9. Summarize the key features of x64dbg and justify its use in malware analysis and reverse engineering. (5)

OR

Summarize the key features of IDA Pro and justify its importance in reverse engineering and malware analysis. (5)

****