HALDIA INSTITUTE OF TECHNOLOGY

(AN AUTONOMOUS INSTITUTION UNDER MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL)

Paper Code: PCC-CS 505

Paper Name: Malware Analysis

Time Allotted: 3 Hours *Full Marks*: 70

The figures in the margin indicate full marks

Candidates are required to give their answers in their own words as far as practicable

Group – A

(Multiple Choice Type Questions)

Choose the correct alternatives from the followings: **15 x 1 = 15**

1. (i) What is the most common method of distributing malware?
a) Social engineering b) Physical media
c) Email attachments d) Website downloads

(ii) What type of malware is designed to steal sensitive information, such as login credentials?
a) Trojan b) Worm c) Ransomware d) Adware

(iii) What is the term for malware that spreads through a network by exploiting vulnerabilities?
a) Adware b) Trojan c) Worm d) Rootkit

(iv) What is the term for malware that gives an attacker remote access to a compromised computer?
a) Worm b) Trojan c) Adware d) Rootkit

(v) What is the term for malware that displays unwanted ads to the user?
a) Worm b) Trojan c) Adware d) Rootkit

(vi) What is the term for malware that is designed to modify or delete files?
a) Trojan b) Worm c) Spyware d) Rootkit

(vii) What type of information can be obtained by analyzing the file header during static analysis?
a) Hash value b) File size c) Encryption key d) IP address

(viii) Which of the following is an indicator of compromise (IoC)?
a) Hash of a suspicious file b) Dynamic analysis report
c) Network traffic logs d) User login history

(ix) Which tool is commonly used for extracting metadata from a suspicious file in static analysis?
a) Wireshark b) IDA Pro c) ExifTool d) Snort

(x) Which of the following is a common file format used in static malware analysis reports?
a) PDF b) PNG c) HTML d) DOCX

(xi) What is the main advantage of dynamic malware analysis over static analysis?
a) Provides real-time behavior of the malware b) Analyzes metadata of the malware
c) Disassembles the malware code d) Identifies file properties and attributes

(xii) Which of the following is an essential component of dynamic malware analysis?
a) Monitoring system calls b) Analyzing file headers
c) Calculating file hashes d) Extracting metadata

(xiii) What is a significant challenge in dynamic malware analysis?
a) Malware evasion techniques b) Extracting metadata
c) Analyzing file headers d) Monitoring system calls

(xiv) What is a key advantage of using a virtual machine in dynamic malware analysis?
a) Isolates the malware from the host system b) Analyzes file metadata
c) Monitors API calls d) Extracts metadata

(xv) Which tool is commonly used for dynamic analysis and reverse engineering of malware?
a) IDA Pro b) Wireshark c) Snort d) OllyDbg

Group – B
(Short Answer Type Questions)

Attempt any three from the followings: **3 x 5 = 15**

2. (i) How can network traffic analysis aid in identifying and understanding the communication patterns of malware within a network?
(ii) What are key differences between static and dynamic malware analysis, and when would you use each approach? 3+2

3. (i) How does dynamic analysis involve executing malware in a controlled environment, and what insights can it provide?
(ii) What are some common techniques used in malware packing, and how do they affect the analysis process? 3+2

4. (i) Explain the concept of packers.
(ii) How they affect static malware analysis. 2+3

5. What is sandboxing, and how is it utilized in dynamic malware analysis? 5

6. Describe the purpose of disassembling in reverse engineering. 5

Group – C
(Long Answer Type Questions)

Attempt any four from the followings: **4 x 10 = 40**

7. (i) What is malware, and what are its main objectives?
(ii) What are the common types of malware?
(iii) How does malware typically spread and infect systems? 5+2+3

8. (i) Explain the significance of behavioral analysis in malware analysis.
(ii) Discuss how observing the behavior of a malware sample in a controlled environment helps in identifying its malicious activities and intentions. 5+5

9. (i) Define static malware analysis.
(ii) Provide a detailed explanation of its importance in the realm of cyber security. 2+8

10. (i) Discuss the importance of monitoring system calls during dynamic malware analysis.
(ii) How does it provide insights into malware activities and intentions? 5+5

11. (i) Discuss the relevance of sandbox evasion techniques in reverse engineering malware.
(ii) Provide examples of evasion mechanisms and ways to counter them. 7+3

12. (i) Discuss the challenges associated with analyzing fileless malware through reverse engineering.
(ii) What are the strategies to overcome these challenges and effectively analyze such malware? 5+5