2204M208

Candidate's Seat No :_____

IMBA in CSM Semester-6 Examination

CSM_BBA_DSE-2

MA

April-2024

Time : 2-30 Hours] **[Max. Marks : 70**

Q.1

A What is malware, and Different types of malwares? How does malware infect devices? (7)

B Difference between static and dynamic malware analysis. (7)

Q.2

A Define the following:(Any Seven) (7)

(1) Exception handling (2) Live malware analysis (3) Dead malware analysis

(4) Trojans (5) Logic bombs (6) Patching (7) Breakpoint (8) Rootkits

(9) Adware

B How does live malware analysis differ from dead malware analysis? (7)

Or

Q.2

A Explain how static analysis tools help in identifying and understanding malware without execution. (7)

B What are the advantages and challenges of conducting live malware analysis? (7)

Q.3

A Explain packet sniffing in Wireshark. (7)

B How can Process Monitor be utilized for monitoring and analyzing the behavior of malware? (7)

Or

Q.3

A Explain signature based malware techniques (7)

B Explain Anti-dynamic analysis techniques. (7)

Q.4

A Define hook injection as a malware technique. Discuss the purpose of hook injection and how it allows malware to manipulate the behavior of a system. (7)

B Explain the primary functionality of downloader malware. (7)

Or

Q.4

A Explain the concept of invariant inference in the context of non-signature- based malware detection. (7)

B How do machine learning methods contribute to malware detection, and what are their limitations? (7)

Q.5

A Explain non-signature-based malware techniques. (7)

B Differentiate between metamorphic and polymorphic malware signatures and their implications for detection. (7)