BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2021/M.Sc.(ANCS)-2022/M.Sc.(ANCS)-2023
Course Name – Malware Analysis and Reverse Engineering
Course Code - MNCS303
(Semester III)

Full Marks : 60 **Time : 2:30 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 15=15

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

(i) Name a disassembler _____.
   a) PE Explorer b) x64dbg
   c) Wireshark d) IDA Pro

(ii) Name a Common Indicator of Compromise _____.
   a) Cross-site-scripting b) DNS Request Anomalies
   c) SQL Injection d) IP Spoofing

(iii) Name a Scanner _____.
   a) Joebox b) Jotti
   c) Wireshark d) YARA

(iv) Tell PEiD used for _____.
   a) for detecting spear phishing b) for identifying hash files
   c) for identifying packers d) for detecting Ip spoofing

(v) Choose Memory analysis performs on _____.
   a) RAM b) ROM
   c) a and b d) None of these

(vi) Solve that RegRipper creates _____ files when it runs.
   a) One b) Two
   c) Three d) None of these

(vii) MAC ACL applies only to _____ packets.
   a) Layer 1 b) Layer 2
   c) Layer 3 d) Layer 4

(viii) Select the online service known for scanning files and URLs using multiple antivirus engines _____.
   a) VirusTotal b) Jotti
   c) NoVirus Thanks d) Threat Expert

(ix) Identify the typical location of Windows Registry hive files _____.

a) C:\Program Files
b) C:\Users
c) C:\Windows\System32\config
d) C:\Temp

(x) Identify the primary function of RegRipper in Registry analysis _____.

a) To destroy Registry hives
b) To change Registry keys
c) To automate data extraction and analysis from the Windows Registry
d) To install software

(xi) Select that what is the purpose of kernel debugging with IDA Pro _____.

a) Debugging web applications
b) Debugging mobile apps
c) Debugging kernel-mode drivers and components
d) Debugging JavaScript code

(xii) What is the primary focus of YARA rules in code analysis _____.

a) To beautify code
b) To identify patterns or characteristics in code
c) To compile code into an executable
d) To debug code

(xiii) What is the primary focus of DLL injection _____.

a) Debugging system issues
b) Extending the functionality of a process
c) Extracting code from an executable
d) Analyzing crash dumps

(xiv) Estimate that what type of analysis can help identify injected code, hidden processes, or suspicious network connections in memory dumps _____.

a) Network analysis
b) Process analysis
c) File system analysis
d) Registry analysis

(xv) Select that code injection involves _____.

a) Extracting code from an executable file
b) Modifying the Windows Registry
c) Inserting and executing code within a running process
d) Decompiling source code

Group-B
(Short Answer Type Questions) 3 x 5=15

2. Describe memory analysis tools used in malware analysis. (3)

3. Describe the purpose of Volatility in malware analysis. (3)

4. Explain the concept of dynamic analysis in the context of REMnux. (3)

5. Explain YARA. (3)

6. Summarize Malfind. (3)

OR

Summarize Recursive DNS query. (3)

Group-C
(Long Answer Type Questions) 5 x 6=30

7. Define Malware Analysis. (5)
8. Describe Static Analysis. (5)

9. Summarize that how Deep Freeze works. (5)

10. Explain PEiD. (5)

11. Express the types of Malware. (5)

12. Explain Sandbox. (5)

OR

Explain INetSim. (5)

****