BRAINWARE UNIVERSITY

Term End Examination 2022
Programme – M.Sc.(ANCS)-2021
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 Common Indicator of Compromise.

a) Cross-site-scripting b) DNS Request Anomalies
c) SQL Injection d) IP Spoofing

(ii) Identify a Malware.

a) Cross-site-scripting b) IP Spoofing
c) Rootkit d) DNS Spoofing

(iii) Identify a Dynamic Analysis Tool for Malware.

a) VirusTotal b) Jotti
c) Regshot d) Threat Expert

(iv) Malware analysis is the process of understanding the behavior of ____________ .

a) Suspicious file b) URL
c) a and b d) None of the above

(v) What is static analysis?

a) Analysing the binary then executing it b) Without executing the binary, analysing it
c) a and b d) None of the above

(vi) Memory analysis performs on ____________.

a) RAM b) ROM
c) a and b d) None of the above

(vii) ASCII stands for __________ .

a) American Static Code for Information Interchange b) American Static Code for Internet Interchange
c) American Structural Code for Information Interchange d) American Standard Code for Information Interchange

(viii) Anubis used for ___ file.

a) Portable executable
b) DLL
c) a and b
d) None of the above

(ix) Dynamic malware analysis executes in ________________.

a) Whitebox
b) Sandbox
c) Blackbox
d) None of the above

(x) Malicious code designed to conceal the existence of other code ________________ .

a) Downloader
b) Rootkit
c) Botnet
d) None of the above

(xi) SHA-1 works with ____ bit hash values.

a) 64
b) 128
c) 256
d) None of the above

(xii) Threat expert provided by ____________.

a) Microsoft
b) Red Hat
c) a and b
d) None of the above

(xiii) Virtual Box developed by ________________.

a) Google
b) Microsoft
c) Oracle
d) None of the above

(xiv) RegRipper extract information from ________________ .

a) registry
b) files
c) a and b
d) None of the above

(xv) Poison Ivy is a __________.

a) Worm
b) Remote Access Trojan
c) Trojan Horse
d) None of the above

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Illustrate Code Injection. (3)
3. Describe WHOIS. (3)
4. Classify Malware Analysis? (3)
5. Focus on JIT debugging. (3)

OR

Explain ACL. (3)

6. Report how Deep Freeze works. (3)

OR

Express the features of Process Monitor. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Define the stages of Reverse Engineering? (5)
8. Classify the types of Malware? (5)
9. Illustrate Basic Static Techniques. (5)
10. Analyse how to discover network and host. (5)
11. Predict how to detect suspicious DLL. (5)

OR

Decide how to detect rootkit with WinDbgScripts. (5)

12. Explain at least three py commands for debugging. (5)

OR

Explain Regshot working. (5)

****