.

Printed Page:-4 **Subject Code:- BCSCY0512**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: V - THEORY EXAMINATION (2025 - 2026)
Subject: Malware Analysis and Reverse Engineering

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*
1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*
2. *Maximum marks for each question are indicated on right -hand side of each question.*
3. *Illustrate your answers with neat sketches wherever necessary.*
4. *Assume suitable data if necessary.*
5. *Preferably, write the answers in sequential order.*
6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

1-a. A malicious program that encrypts files and demands payment for decryption is categorized as. (CO1,K1) 1

(a) Worm
(b) Rootkit
(c) Trojan
(d) Ransomware

1-b. Email attachments requiring user interaction to execute are often linked with. (CO1,K1) 1

(a) Trojan
(b) Worm
(c) Adware
(d) Spyware

1-c. The default executable file format for Windows operating systems is. (CO2, K1) 1

(a) PE
(b) ELF
(c) Mach-O
(d) DEX

1-d. The "Magic Number" in file headers is used to. (CO2, K2) 1

(a) Identify file type
(b) Encrypt files
(c) Check permissions
(d) Compress data

.

1-e. Identify the VirtualBox networking mode that isolates the VM from the external internet while allowing host-to-VM communication. (CO3,K1) 1

(a) NAT
(b) Bridged
(c) Host-only
(d) Internal Network

1-f. Monitor logs that capture detailed file, registry and process activity are produced by: (CO3,K2) 1

(a) Process Explorer
(b) TCPView
(c) Process Monitor
(d) FakeNet-NG

1-g. In x86 architecture, the register primarily used for stack operations is? (CO4, K2) 1

(a) EAX
(b) ESP
(c) EBX
(d) ECX

1-h. Using IDA Pro, the feature that helps recover function boundaries is called? (CO4,K2) 1

(a) Hex view
(b) Function listing
(c) String search
(d) Auto-analysis

1-i. Identify the technique that injects a DLL into another process to run code in that process's context.(CO5, K2) 1

(a) DLL injection
(b) API hooking
(c) Code obfuscation
(d) Memory dumping

1-j. During IOC extraction, which artifact type is an example of a network-based IOC? (CO5,K1) 1

(a) IP address
(b) Registry key
(c) File hash
(d) File path

2. Attempt all parts:-

2.a. Define malware with suitable example. (CO1, K1) 2

2.b. Identify the main functionality of Detect It Easy (DIE). (CO2, K2) 2

2.c. List two differences between VirtualBox and VMware relevant to malware analysis. (CO3,K1) 2

2.d. Explain the role of the MOV instruction. (CO4,K2) 2

2.e.	Define DLL injection and give one common use-case for it. (CO5,K1)	2

SECTION-B 30

3. Attempt all parts:-

3.a. Answer any one of the following:-

3.a.(i)	State the main contribution of signature-based detection in antivirus systems. (CO1,K1)	6
3.a.(ii)	Discuss the working and impact of ransomware on organizations. (CO1, K2)	6

3.b. Answer any one of the following:-

3.b.(i)	Analyze the differences between PE and ELF file formats in terms of structure and attributes. (CO2, K2)	6
3.b.(ii)	Analyze the advantages and disadvantages of using YARA rules in threat hunting. (CO2, K3)	6

3.c. Answer any one of the following:-

3.c.(i)	Describe the process of capturing and filtering traffic in Wireshark to isolate a sample's HTTP communications. (CO3, K2)	6
3.c.(ii)	Explain how Cuckoo Sandbox executes and collects behavioral artifacts from a sample (high level). (CO3, K3)	6

3.d. Answer any one of the following:-

3.d.(i)	Describe the internal structure and operation of x86 registers during program execution. (CO4, K2)	6
3.d.(ii)	Illustrate the difference between direct and indirect calls in assembly. (CO4, K2)	6

3.e. Answer any one of the following:-

3.e.(i)	Explain three different DLL injection techniques (briefly describe each). (CO5, K2)	6
3.e.(ii)	Describe how anti-debugging techniques can be implemented in user-mode malware and propose three ways an analyst can bypass or neutralize these techniques during analysis. (CO5, K3)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Provide a detailed analysis of viruses, worms, and Trojans with real examples. (CO1, K1)	10
4-b.	Examine the implications of cyber warfare in critical infrastructure attacks. (CO1, K2)	10

5. Answer any one of the following:-

5-a.	Explain how file entropy analysis helps in identifying packed malware. (CO2, K2)	10
5-b.	Analyze a scenario where a PE file is suspected to be malicious and describe the step-by-step process of analyzing its header, imports, and sections using PEStudio, PEiD, and Detect It Easy. (CO2, K3)	10

6. Answer any one of the following:-

6-a.	Critically evaluate the pros and cons of using VirtualBox versus VMware for advanced malware analysis labs (consider features, performance, detection surface and licensing). (CO3, K3)	10
6-b.	Develop a comprehensive methodology for correlating Process Monitor events,	10

.

Process Explorer observations, and packet captures to produce an accurate attack timeline. (CO3, K4)

7. Answer any one of the following:-

7-a.	Analyze the different types of x86 registers and their participation in the program execution cycle. (CO4, K4)	10
7-b.	Elaborate on how dynamic analysis complements static disassembly in malware examination. (CO4, K3)	10

8. Answer any one of the following:-

8-a.	Provide a detailed explanation of DLL injection mechanics. Include at least four injection methods (e.g., CreateRemoteThread, SetWindowsHookEx, APC, Reflective DLL injection), how they work at a technical level, the memory artifacts they leave, and detection strategies for each. (CO5, K3)	10
8-b.	Construct a template for a professional malware analysis report aimed at technical stakeholders. Include sections, required technical appendices (hashes, YARA rules, Volatility output snippets), and a concise mitigation and detection roadmap. (CO5, K4)	10