

Question 1 Answer the following questions:

- i. Compare and contrast vulnerability management and vulnerability assessment. 7Marks
How do the stages of vulnerability management interrelate with VAPT activities?
- ii. Describe the phases and methodologies of penetration testing. Provide a scenario 7Marks
and indicate which methodology you would choose and why.

OR

- i. Explain in detail the prerequisites and best practices to conduct a vulnerability scan 7Marks
on a production system.
- ii. "False positives are a major challenge in vulnerability scanning." Discuss and 7Marks
explain techniques to reduce or filter false positives effectively.

Question 2 Answer the following questions:

- i. A client wants you to perform both vulnerability assessment and penetration testing 7Marks
of their web application infrastructure. Outline a full methodology, tools, and
deliverables you would use.
- ii. Write a detailed note on Metasploit: architecture, modules, workflows, and 7Marks
advanced features.

OR

- i. What is port scanning? Explain common port scanning techniques and how 7Marks
defenders can detect and defend against scanning.
- ii. Elaborate on how buffer overflow vulnerabilities are discovered, exploited, and 7Marks
mitigated. Include stack-based and heap-based examples.

Question 3 Answer the following questions:

- i. Discuss how you would structure a sample penetration test report, including 7Marks
sections, content, evidence, and presentation strategy.
- ii. You are given a report showing multiple critical vulnerabilities on a host. Describe 7Marks
how you would analyze, prioritize, and communicate to management & technical
teams.

OR

V 849-2

- i. Explain social engineering attacks in detail. Provide examples, countermeasures, and how such attacks integrate in a full penetration test. 7Marks
- ii. Explain static code analysis and reverse engineering as techniques in VAPT. How do they complement dynamic testing? 7Marks

Questions 4 Answer the following questions:

- i. Discuss in detail the kinds of penetration testing (web, network, client-side, physical, social engineering), with tools and techniques used for each. 7Marks
- ii. Explain the architecture and core components of Burp Suite and describe the role of each component in web application testing. 7Marks

OR

- i. Discuss compliance requirements in the context of vulnerability assessment and how scan policies can be tailored to verify compliance 7Marks
- ii. Given a case study: A web server hosts sensitive financial data. The scanner reports directory traversal, SQL injection, and an outdated SSL protocol. As a penetration tester, describe your step-by-step approach from vulnerability verification through exploitation to remediation recommendations. 7Marks

Questions 5: Attempt any Seven out of Twelve.

14 Marks

1. Describe the significance of test cases or scenarios in planning a penetration test.
2. Describe how intrusion detection tools can be bypassed during penetration testing.
3. Explain the role of false positive analysis in vulnerability management.
4. Discuss compliance requirements and their impact on vulnerability assessment.
5. How does compliance checking differ across operating systems and databases? Explain with examples.
6. Compare and contrast black box, white box, and fuzz testing methodologies in penetration testing.
7. Describe how penetration testing differs when targeting hardware as opposed to software.
8. How is a sample penetration test report structured? Highlight key sections.
9. Differentiate between active and passive reconnaissance with examples of tools used.
10. Discuss different types of penetration testing with real-world examples.
11. Describe how Wireshark aids in analyzing network services during penetration testing.
12. Discuss the impact of social engineering attacks during the information gathering phase.

.....X.....X.....

2511N849 -3

Candidate's Seat No : _____

IMSc (CSF) Sem.-9 Examination

ICSF-503 (EB)

Malware Analysis

November-2025

Time : 2-30 Hours]

[Max. Marks : 70

Question 1 Answer the following questions:

- i. You receive a security alert indicating that a known system process (explorer.exe) is executing unfamiliar instructions, yet no new process appears in the task manager. The behavior is stealthy and persistent. Identify and explain technique allows such code execution. 7Marks
- ii. What is fileless malware? How does it leverage LOLBins to avoid detection and persist within a system? Describe the steps involved from initial access to execution. 7Marks

OR

- i. Explain command and Control (C2) infrastructure in malware communication. Describe the methods used by malware to establish and maintain C2 communication channels. 7Marks
- ii. How is an ELF file structured, and what roles do its main components play during execution? In what ways can attackers misuse its sections for malicious activity? 7Marks

Question 2 Answer the following questions:

- i. During memory forensics, a DLL is loaded inside lsass.exe, yet its export table lists only one function that runs instantly on load. Explain what chain of operations likely brought that DLL there and why its entry routine becomes the perfect hiding spot. 7Marks
- ii. A sample deliberately produces decompiler output full of meaningless branches that never alter program state. Explain concept. Describe how you would prove these branches are spurious and recover the underlying logic in a defensible way. 7Marks

OR

- i. An executable resolves API functionality only at runtime and avoids leaving readable names in its tables. Explain a rigorous method to map those runtime references back to known interfaces and how you would confirm your mappings are correct. 7Marks
- ii. An analyst sees return addresses that point into short snippets across modules rather than a single payload region. Explain what this layout implies and list the 7Marks

investigative artifacts you would extract to support a technical finding.

Question 3 Answer the following questions:

- i. A multinational energy company's field devices begin failing simultaneously after receiving a legitimate over-the-air update. Explain how a malware actor could have manipulate this update mechanism and describe the forensic steps to confirm and contain the compromise. 7Marks
- ii. Differentiate between Modbus and DNP3 protocols in terms of communication efficiency, error handling, and reliability. 7Marks

OR

- i. In a research simulation, analysts deploy smart-city devices using HTTP/HTTPS for cloud communication, Zigbee for sensor connectivity, and LoRaWAN for long-range telemetry. Describe the layered security challenges this mixed environment introduces. 7Marks
- ii. Explain data logger, describe its working mechanism, and explain how it supports real-time data acquisition in SCADA systems. 7Marks

Questions 4 Answer the following questions:

- i. Explain the Activity lifecycle in Android. 7Marks
- ii. Explain the process of extracting, decoding, and rebuilding an APK using common analysis tools. 7Marks

OR

- i. Describe the complete internal structure of a DEX file and explain the purpose of each section. 7Marks
- ii. A DEX file references hidden native libraries under `/lib/armeabi-v7a/`. Explain how JNI bridging allows malware to execute native payloads. 7Marks

Questions 5: Attempt any Seven out of Twelve.

14 Marks

1. Explain why heterogeneous IoT ecosystems challenge uniform patch-management policies.
2. Why is binary entropy analysis useful in detecting packed executables even without signatures?
3. How can analyzing NtQueueApcThread behavior expose stealthy inter-process payload transfers?
4. What role do CPUID vendor strings and MAC prefixes play in scalable sandbox fingerprinting?
5. How can combining sandbox network captures with static YARA signatures yield stronger

N849.5

attribution evidence?

6. When a thread repeatedly invokes WaitForSingleObjectEx, what kind of attacker-controlled routine can exploit this state?
7. Why do kernel-level rootkits pose greater persistence risks than user-space ones? Explain both.
8. Which code transformation technique changes MOV EAX, 10 into an equivalent but obfuscated form? Give example.
9. In Android malware, what evidence in the manifest-DEX relationship suggests privilege escalation? Give example
- 10 What is AtomBombing?
- 11 What is timing analysis in anti-debugging techniques?
- 12 A forensic analyst finds frequent calls to ZwUnmapViewOfSection followed by VirtualAllocEx. Which attack pattern might this indicate?

.....X.....X.....