5/21

2511N850

Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination
CSM-MBA-503 (EA)
VAPT
November-2025

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

Question 1 Answer the following questions:

i. Compare and contrast vulnerability management and vulnerability assessment. How do the stages of vulnerability management interrelate with VAPT activities? 7Marks

ii. Describe the phases and methodologies of penetration testing. Provide a scenario and indicate which methodology you would choose and why. 7Marks

OR

i. Explain in detail the prerequisites and best practices to conduct a vulnerability scan on a production system. 7Marks

ii. "False positives are a major challenge in vulnerability scanning." Discuss and explain techniques to reduce or filter false positives effectively. 7Marks

Question 2 Answer the following questions:

i. A client wants you to perform both vulnerability assessment and penetration testing of their web application infrastructure. Outline a full methodology, tools, and deliverables you would use. 7Marks

ii. Write a detailed note on Metasploit: architecture, modules, workflows, and advanced features. 7Marks

OR

i. What is port scanning? Explain common port scanning techniques and how defenders can detect and defend against scanning. 7Marks

ii. Elaborate on how buffer overflow vulnerabilities are discovered, exploited, and mitigated. Include stack-based and heap-based examples. 7Marks

Question 3 Answer the following questions:

i. Discuss how you would structure a sample penetration test report, including sections, content, evidence, and presentation strategy. 7Marks

ii. You are given a report showing multiple critical vulnerabilities on a host. Describe how you would analyze, prioritize, and communicate to management & technical teams. 7Marks

OR

P.T.O

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 (e.g. PCI-DSS, ISO 27001) 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.....

2511N850 ← 3 Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination
CSM-MBA-503 (EB)
Malware Analysis
November-2025

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

Question 1 Answer the following questions:

i. Explain how container-based malware infiltrates and operates within Docker or Kubernetes environments and discuss key indicators of compromise along with effective security measures. 7Marks

ii. A disassembler shows many jumps to empty or unused labels in the code. What could this indicate about instruction flow obfuscation, and how would it affect analyzing of the program? 7Marks

OR

i. An analyst runs a packed malware sample in a virtual sandbox but fails to see post-decryption behavior. Explain procedure to unpack the malware in a live analysis environment. 7Marks

ii. Explain the working mechanism of virtualization-based obfuscation. How does it hinder reverse engineering efforts. 7Marks

Question 2 Answer the following questions:

i. While analyzing a sample, every conditional appears to funnel into the same handler and many bytes look meaningless. Explain a methodical approach to reveal the program's true execution paths. 7Marks

ii. Analysts detect raw opcodes inside a process with no matching module on disk, but the code still executes after address randomization. Explain the loading style this represents and why such code survives despite layout changes. 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 investigative artifacts you would extract to support a technical finding. 7Marks

P.T.O

N 850- 4

Question 3 Answer the following questions:

i. A malware analyst is asked to investigate a malicious sample found in a router that runs on a RISC-based processor. The binary doesn't match typical x86 instructions. Discuss what characteristics of the processor architecture could lead to this mismatch. 7Marks

ii. 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

OR

i. Explain the concept of firmware, its role in embedded devices, and how it enables hardware–software interaction. 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?

N8501.5

5. How can combining sandbox network captures with static YARA signatures yield stronger attribution evidence?
6. When a thread repeatedly invokes WaitForSingleObjectEx, what kind of attacker-controlled routine can exploit this state?
7. How can analyzing the method_ids section reveal dynamic code-loading behavior?
8. Why do firmware infections resemble bootloader compromises in mobile malware?
9. Explain the full VirtualAllocEx → WriteProcessMemory → CreateRemoteThread sequence and the typical preconditions required.
10 Why are Early-Bird APC attacks harder to intercept than ordinary remote-thread injections?
11 How can malformed SEH chains be both a crash symptom *and* an exploitation vector?
12 Why is firmware-level authentication often ignored in consumer IoT but enforced in industrial SCADA?

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