7/71

1511E1253

Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

503

Cyber Security & Forensics (EA)

Time : 2-30 Hours] November-2025 [Max. Marks : 70

Question 1 Answer the following questions:

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

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

OR

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

Question 2 Answer the following questions:

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

Question 3 Answer the following questions:

i. 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

ii. Explain static code analysis and reverse engineering as techniques in VAPT. How do they complement dynamic testing? 7Marks

OR

i. Explain social engineering attacks in detail. Provide examples, countermeasures, 7Marks

P.T.O

and how such attacks integrate in a full penetration test.

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

Questions 4 Answer the following questions:

i. 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 The scanner reports directory traversal, SQL injection, and an outdated SSL protocol.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

ii. 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

OR

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 describethe role of each component in web application testing. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. Differentiate between active and passive reconnaissance with examples of tools used.
2. Discuss the impact of social engineering attacks during the information gathering phase.
3. Discuss compliance requirements and their impact on vulnerability assessment.
4. Explain the role of false positive analysis in vulnerability management.
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. Describe the significance of test cases or scenarios in planning a penetration test.
10. Discuss different types of penetration testing with real-world examples.
11. Describe how Wireshark aids in analyzing network services during penetration testing.
12. Describe how intrusion detection tools can be bypassed during penetration testing.

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

1511E1253 —3 Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

503

Cyber Security & Forensics (EB)

November-2025

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

Question 1 Answer the following questions:

i. Explain what compiler optimizations are and why they are crucial in binary analysis. Distinguish between high-level and low-level compiler optimizations with examples. 7Marks

ii. Describe the internal structure of a Portable Executable (PE) file. Explain the purpose of each major component. How are sections exploited or manipulated by attackers? 7Marks

OR

i. Analyze how modern malware detects execution within virtual machines. Discuss the forensic challenges posed by anti-VM techniques. 7Marks

ii. Elaborate on the role of system call hooking and API redirection in advanced malware. How do these techniques interfere with normal OS behavior? 7Marks

Question 2 Answer the following questions:

i. 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

ii. An idle thread executes injected logic only after a normal system API call puts it into a waiting state. Explain how this delayed execution mechanism works, why it avoids breakpoints, and what events would trigger it. 7Marks

OR

i. Decompiled output from one function looks mathematically absurd branches never change results, but execution paths loop unpredictably. Explain the obfuscation principles combined here and suggest how an investigator could restore readability. 7Marks

ii. Static analysis fails to resolve imported calls because destinations are computed at runtime. Explain the reason malware uses such indirection and give one static and one dynamic way to uncover the true call graph. 7Marks

P.T.O

E1253-4

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. Explain the concept of firmware, its role in embedded devices, and how it enables hardware–software interaction. 7Marks

OR

i. Compare Mirai, Bashlite, Hajime, and Mozi botnets in terms of their communication models, infection methods, and capabilities. 7Marks

ii. You are tasked with designing a defense plan for a heterogeneous IoT ecosystem (sensors, gateways, and cloud). Using your understanding of IoT architecture, propose a layered mitigation framework that addresses likely malware attack points from the physical to the application level. 7Marks

Questions 4 Answer the following questions:

i. A malware sample mimics a banking app. Explain how you would analyze its APK and DEX components to confirm it's a trojan. 7Marks

ii. Describe the complete internal structure of a DEX file and explain the purpose of each section. 7Marks

OR

i. Explain the Android architecture in detail. Describe each layer with suitable example. 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. Why are Early-Bird APC attacks harder to intercept than ordinary remote-thread injections?
2. How can malformed SEH chains be both a crash symptom *and* an exploitation vector?
3. When comparing explorer.exe in memory and on disk, which evidence would confirm process hollowing rather than reflective loading?
4. Why can function-pointer obfuscation break IDA's call-graph reconstruction but not dynamic tracing?
5. Why is firmware-level authentication often ignored in consumer IoT but enforced in industrial SCADA?

E1253-5

6. What evidence in AndroidManifest.xml suggests privilege escalation via exported components?
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 What is AtomBombing?
11 What is timing analysis in anti-debugging techniques?
12 What is position-independent code (PIC)?

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

P.T.O

1511E1253 –6 Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

503

Cyber Security & Forensics (EC)

Time : 2-30 Hours] November-2025 [Max. Marks : 70

Question 1 Answer the following questions:

i. Define IoT and describe its core characteristics. 7Marks

ii. Detail the physical design of IoT, focusing on hardware components and device integration. 7Marks

OR

i. Compare and contrast different IoT levels and deployment models. 7Marks

ii. Explain the role of sensors, actuators, cloud computing, big data, and AI in enabling IoT. 7Marks

Question 2 Answer the following questions:

i. Explain Machine-to-Machine (M2M) communication and its management. 7Marks

ii. Describe the role of SDN and NFV in IoT network management. 7Marks

OR

i. Compare hardware/software communication standards: UART, SPI, I2C, and JTAG. 7Marks

ii. Discuss network management challenges in large-scale IoT deployments. 7Marks

Question 3 Answer the following questions:

i. Define SCADA and describe its role in Industrial Control Systems (ICS). 7Marks

ii. Describe the Purdue model of SCADA and its components. 7Marks

OR

i. Analyze SCADA applications in industries and typical threats faced. 7Marks

ii. Explain the architecture and working of field devices and control units in SCADA. 7Marks

Questions 4 Answer the following questions:

i. Compare Modbus, DNP3, and PROFIBUS protocols with their vulnerabilities. 7Marks

ii. Explain the Defense-in-Depth model in ICS/SCADA environments. 7Marks

OR

i. Propose a penetration testing strategy tailored for ICS environments. 7Marks

ii. Discuss incident response and reporting process after SCADA penetration testing. 7Marks

E 1253-7

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. What is the role of cloud computing in IoT?
2. Expand M2M and explain its meaning in one line.
3. Define interoperability in the context of IoT.
4. Write any one difference between IoT and M2M.
5. Expand NFV and state its purpose.
6. Write the full form of UART and SPI.
7. What is the main function of a SCADA system?
8. Give one example of a SCADA application in industry.
9. List any two differences between IT and OT systems.
10 What is ladder logic?
11 What is the purpose of penetration testing in ICS?
12 What is the difference between active and passive testing?

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