5/51

2211E796

Candidate's Seat No :_____

M.Sc Sem-3 Examination

503

Cyber Security & Forensic (EA)

November-2024

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

Question 1 Answer the following questions:

i. What are "Injection" vulnerabilities in web applications, and what are common types of injection attacks? Describe these vulnerabilities and discuss methods for mitigating them. 7Marks

ii. Define Cross-Site Scripting (XSS) and describe the various types of XSS attacks. How does each type differ in terms of execution and impact? 7Marks

OR

i. What are the risks associated with "Broken Authentication" in web applications? Provide examples of common vulnerabilities and outline best practices for implementing secure authentication mechanisms. 7Marks

ii. How can an attacker exploit a reflected XSS vulnerability? Provide a step-by-step example to illustrate how this type of attack is executed. 7Marks

Question 2 Answer the following questions:

i. What is Metasploit and how is it used in vulnerability exploitation? Provide a brief overview of its functionalities. 7Marks

ii. Explain the concepts of buffer overflow and fuzzing in the context of vulnerability exploitation. Why are they significant? 7Marks

OR

i. What are the key components of compliance reporting in vulnerability management? How do they relate to security policies? 7Marks

ii. What is the role of Nessus in vulnerability assessment, and what are its main features and benefits? Discuss how Nessus supports effective security management. 7Marks

Question 3 Answer the following questions:

i. What are Black Box, White Box, and Grey Box testing methodologies in penetration testing, and how does each approach differ in its advantages and limitations? 7Marks

ii. Describe how end-user behavior can be tested in penetration testing. What methods can be employed? 7Marks

OR

i. What tools are commonly used in penetration testing? Compare at least three tools, highlighting their specific applications and features. 7Marks

ii. Explain how penetration testing can be applied to software applications. What specific vulnerabilities should be assessed? 7Marks

(P.T.O)

E796-2

Questions 4 Answer the following questions:

i. Compare the different types of penetration testing: Social Engineering, Web Application, Physical, Network Services, and Client-side tests. What are the unique challenges of each? 7Marks

ii. Explain the role of Wireshark in network penetration testing. How can it be used to identify security issues? 7Marks

OR

i. Discuss the impact of case studies on the understanding of penetration testing. What can be learned from real-world examples? 7Marks

ii. What are the best practices for conducting a social engineering test? How can organizations prepare for such tests? 7Marks

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What is the primary purpose of vulnerability assessment?
2. What is vulnerability assessment?
3. Given a target system, conduct active information gathering by identifying open ports using Nmap. What command would you use?
4. What is the first step in the vulnerability assessment life cycle? Why?
5. What is remediation in vulnerability management?
6. What does "false positive" mean in vulnerability scanning?
7. How is vulnerability exploitation conducted?
8. Differentiate between fuzz testing and black-box testing.
9. What is the function of Wireshark?
10. What is risk severity applicability analysis?
11. How would you use Nmap to discover hosts in a network?
12. Use Acunetix to scan a web application. What steps would you take?

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

2211E796-3 Candidate's Seat No :_____

M.Sc Sem-3 Examination

503

Cyber Security & Forensic (EB)

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Define malware and explain its different types with examples. 7Marks

ii. What steps are involved in setting up a malware analysis laboratory, and what tools are essential 7Marks

OR

i. Explain the different types of malware and their characteristics. How do these characteristics influence the approach taken during analysis? 7Marks

ii. Discuss the importance of setting up a malware analysis laboratory. What key components and tools should be included, and why are they critical for effective analysis? 7Marks

Question 2 Answer the following questions:

i. Explain the significance of memory forensics in malware analysis and describe extracting and analysing artefacts from memory dumps. 7Marks

ii. Discuss the techniques for identifying and analyzing rootkits within a system. Why are rootkits particularly challenging to detect in malware investigations? 7Marks

OR

i. Describe the process of extracting and analyzing artifacts from memory dumps. What tools and techniques are essential for this task, and what types of information can be retrieved? 7Marks

ii. Explain the challenges associated with reversing obfuscated binaries. What advanced techniques can be employed to overcome these challenges, particularly with respect to self-modifying code? 7Marks

Question 3 Answer the following questions:

i. Explain the differences between static and dynamic malware analysis techniques. 7Marks

ii. Describe the use of YARA signatures in malware detection. How do they differ from Clam AV Virus signatures? 7Marks

OR

i. Analyze the significance of understanding Tactics, Techniques, and Procedures (TTPs) used by Advanced Persistent Threats (APTs). How does this knowledge assist in the detection and mitigation of APT attacks? 7Marks

ii. Discuss the implications of analyzing living-off-the-land attacks. What strategies can be used to detect and respond to such attacks, and why are they particularly challenging to analyze? 7Marks

Questions 4 Answer the following questions:

i. Explain how PE (Portable Executable) file headers and sections can provide insights into malware behaviour. 7Marks

(P.T.O)

ii. Describe the forensic importance of malware analysis in digital forensics investigation 7Marks

OR

i. What is process injection in malware, and why is it used? Provide examples of how this behavior can be detected during an analysis 7Marks

ii. What is memory-resident malware, and how does it differ from traditional malware? Give an example of how an analyst might detect memory-resident malware during an investigation. 7Marks

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What is malware?
2. Name two types of malware.
3. Why is malware analysis important in digital forensics?
4. What is static analysis in the context of malware analysis?
5. What does hash help achieve in malware analysis?
6. What is the purpose of using sandboxes in dynamic malware analysis?
7. Name one tool used for decoding obfuscated strings during static analysis.
8. What tool does Wireshark use in malware analysis?
9. What is the function of PE (Portable Executable) file headers in malware analysis?
10. What are YARA signatures used for in malware detection?
11. What is the importance of malware analysis in cybersecurity?
12. Describe one static and dynamic analysis technique used in malware analysis.

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

2211E796-5 Candidate's Seat No :_____

M.Sc Sem-3 Examination

503

Cyber Security & Forensic (EC)

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Describe the standardized architecture of the oneM2M IoT framework. 7Marks
ii. Discuss the benefits of IoT applications in Connected Roadways, Connected Factories, and Smart Cities. 7Marks

OR

i. What are the main challenges in ensuring IoT security? 7Marks
ii. Explain the role and functionality of the Communications Network Layer in a simplified IoT architecture. 7Marks

Question 2 Answer the following questions:

i. Define smart objects in IoT and explain their communication requirements. 7Marks
ii. Differentiate between Direct Sequence Spread Spectrum (DSSS) and Parallel Sequence Spread Spectrum (PSSS) technologies. 7Marks

OR

i. Explain IEEE 802.15.4 as an IoT access technology and its relevance. 7Marks
ii. Describe the MQTT protocol and its application at the IoT application layer. 7Marks

Question 3 Answer the following questions:

i. Illustrate the structure of SCADA systems, highlighting its key components. 7Marks
ii. Discuss the benefits of customization as a feature in SCADA systems. 7Marks

OR

i. Explain the deployment of a multi-level SCADA architecture. 7Marks
ii. How have SCADA systems evolved over successive generations? 7Marks

Questions 4 Answer the following questions:

i. Describe a Remote Terminal Unit (RTU) and its essential components in detail. 7Marks
ii. Illustrate the importance of Human-Machine Interface (HMI) in a SCADA system. 7Marks

OR

i. Explain the Modbus protocol and its working mechanism. 7Marks
ii. Explain SCADA Servers and Control Panels and their key features. 7Marks

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What is Ladder Logic Programming?
2. What is Resistive touchscreens HMI?
3. What is Analog and Digital Signalling?
4. Give any 2 applications of SCADA.
5. Describe First Generation SCADA system in brief.
6. Define Invasive Sensors, Non-Invasive Sensors, Absolute Sensors, Relative Sensors.
7. Explain the Data Management in SCADA in short.
8. What is Beacon Synchronization?
9. Give some examples of pressure sensors.
10. Give any 2 examples of medium range communication protocols used in IoT.
11. Give any 4 features of 6LoWPAN.
12. Describe QoS and its levels.