0502E1474

Candidate's Seat No : _____

MSc Sem.-1 Examination

404

Cyber Security & Forensics

February-2025

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

Question 1 Answer the following questions:

i. A developer is considering building an Android application and wants to understand the evolution of Android from its inception to its current state. Discuss the major milestones that shaped its development and features. 7Marks

ii. A smartphone manufacturer is designing a new device and wants to ensure seamless customer experience. Explain how Android's hardware and software architecture work together to achieve this goal. 7Marks

OR

i. A cybersecurity team is tasked with evaluating an Android device's security. Describe the Android security model and its role in safeguarding user data and system integrity. 7Marks

ii. A team is developing a sensitive application and is debating the use of Android's permission model. Explain how this model protects user privacy and prevents unauthorized access. 7Marks

Question 2 Answer the following questions:

i. A tech company is analyzing how iOS has evolved to influence its current features and functionality. Highlight the key upgrades and advances in iOS over time. 7Marks

ii. An iOS development team wants to understand how the iOS architecture supports safe and efficient operation. Explain the essential components and their collaboration between hardware and software. 7Marks

OR

i. A government agency is deploying iOS devices for secure communication. Describe the iOS security model and how it protects user data's confidentiality, integrity, and availability. 7Marks

ii. A developer is designing an iOS app that accesses sensitive user data. Explain the iOS permissions model and provide examples of how it regulates access to such data. 7Marks

Question 3 Answer the following questions:

i. A security analyst is setting up an environment for mobile application penetration testing. Discuss the critical elements required to create this environment and ensure accurate and secure testing. 7Marks

ii. During a penetration test, an analyst wants to exploit potential vulnerabilities in mobile devices. Explain how proper engagement with these devices aids in identifying and exploiting such vulnerabilities. 7Marks

OR

i. Explain the process of setting up a virtual environment for mobile application penetration testing. 7Marks

(P.T.O)

ii. Explain how Burp Suite is used for traffic interception in mobile application penetration testing. 7Marks

Questions 4 Answer the following questions:

i. A cybersecurity consultant is investigating client-side injection vulnerabilities in a mobile app. Explain the risks, exploitation methods, potential consequences, and mitigation strategies. 7Marks

ii. A financial app developer is concerned about improper session handling mechanisms. Discuss how attackers might exploit this vulnerability and suggest effective mitigation techniques. 7Marks

OR

i. Describe the step-by-step process of configuring a live device for penetration testing, including hardware and software requirements. 7Marks

ii. Discuss the general steps in developing a mitigation approach for identified vulnerabilities in mobile application security. 7Marks

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

1. Which file in an Android application contains permissions and application components?
2. How does sandboxing prevent unauthorized access in Android and iOS applications?
3. What is the primary purpose of code signing in mobile applications?
4. What vulnerability arises from hardcoded cryptographic keys in a mobile app?
5. What are the security risks of rooting Android or jailbreaking iOS devices?
6. What is the primary purpose of sandboxing in Android and iOS applications?
7. What common risk is associated with insufficient transport layer protection in mobile apps?
8. What is the role of the Keychain in iOS security?
   A. To store sensitive user data securely
   B. To manage application permissions
   C. To improve application performance
   D. To debug applications
9. Which tool is commonly used for traffic interception in mobile penetration testing?
   A. Burp Suite B. Drozer
   C. Wireshark C. Nessus
10. How does the Android security model protect user data and application integrity?
    A. By encrypting all user data
    B. By using a permission-based access control system
    C. By isolating app processes through sandboxing
    D. By implementing regular application updates
11. Why are proper session handling mechanisms important in mobile applications?
    A. To reduce application load times
    B. To ensure secure communication between the user and the server
    C. To improve overall application performance

D. To enable access to debugging logs

12 What is the primary difference between Android and iOS in hardware and software architecture?

A. Android relies on proprietary hardware, iOS uses open-source hardware
B. Android uses monolithic architecture, iOS employs modular design
C. Android supports varied hardware, iOS is restricted to Apple's hardware
D. iOS includes virtual machines, Android does not

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