Seat No.: _____ Enrolment No. 2013

NATIONAL FORENSIC SCIENCES UNIVERSITY

M. Sc. Cyber Security
Semester – II – July - 2024

Subject Code: CTMSCS SII P3 **Date:** 12/07/2024
Subject Name: Mobile Security
Time: 02:30 PM to 05:30 PM **Total Marks:** 100

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

		Marks
Q.1	**Answer the following (Attempt Any Three)**	
(a)	You have discovered that an Android application has several unpatched vulnerabilities listed in the OWASP Top 10. Using dynamic analysis tools such as MobSF and Frida, explain how you would go about exploiting these vulnerabilities. Provide a detailed plan on how you would document the findings and propose fixes to the development team.	**08**
(b)	You have been hired by a financial institution to conduct a comprehensive security audit of their newly developed Android banking application. The application handles sensitive financial transactions and user data. Outline a detailed approach for performing both static and dynamic analysis of the application using tools like MobSF, Drozer. Explain how you would identify potential security flaws, assess their impact, and recommend remediation steps to ensure the application's security.	**08**
(c)	Discuss the steps involved in the Android boot process and their security implications.	**08**
(d)	Describe the importance of reverse engineering in Android Application Security and importance of secure source code review in Android application security	**08**
Q.2	**Answer the following (Attempt Any Three)**	
(a)	During a routine security audit, you suspect that an Android application is leaking sensitive user data over the network. Describe the steps you would take to perform traffic analysis using tools like Wireshark and HTTP Proxy Interception. Explain how you would identify and mitigate any data leaks found during your analysis.	**08**
(b)	How can Drozer be used for security auditing in Android applications?	**08**

(c) Explain the architecture of Android. 08

(d) What is insecure login and how can it be exploited in Android applications? 08

Q.3 Answer the following (Attempt Any Three)

(a) What is the Android Run Time (ART) and its importance? Also discuss the purpose of ARM Translator in Android security? 08

(b) Discuss the common input validation issues in Android applications. 08

(c) What are client-side injection attacks, and how do they affect Android applications? 08

(d) Explain the concept of Android partitions and their significance in security. 08

Q.4 Answer the following (Attempt Any Two)

(a) Describe the role of ADB commands in Android application pen-testing by taking atleast 5 ADB Commands. 07

(b) Discuss the strategy for mobile application security pen-testing. 07

(c) Describe the process of traffic analysis for Android devices and its significance in security. 07

Q.5 Answer the following (Attempt Any Two)

(a) You are tasked with pen-testing a newly developed Android application. The app includes features like user authentication, data storage, and API communication. Describe the steps you would take to identify and exploit potential vulnerabilities in this application. Include the tools and techniques you would use. 07

(b) A company's proprietary Android app has been leaked online, and you are assigned to assess the potential security risks involved. Explain how you would use reverse engineering tools like (JD-GUI, Hex-Dump, etc..) to analyze the app's code and identify any sensitive information or vulnerabilities that might have been exposed. 07

(c) Describe the use of APKTool in reverse engineering Android applications in detail. 07

--- End of Paper---