Day 24

Topic: Mobile Security

Objective: To analyze the security architecture of mobile operating systems and common threats.

Theoretical Concepts:
We examined the Android permission model and the concept of "Sandboxing" apps. We discussed OWASP Mobile Top 10 risks, including Insecure Data Storage and Extraneous Functionality.

Practical Work:
We set up an Android Emulator (Genymotion). We used **MobSF (Mobile Security Framework)**, an automated analysis tool. We uploaded a sample APK file to MobSF, which performed a static analysis, revealing hardcoded API keys and insecure permissions in the manifest file.

Tools Used: Android Emulator, MobSF.

Outcome: Ability to perform static analysis on Android applications to find security flaws.