**Process to identify mobile application architecture and connected services**

| **Step** | **Action** | **Tools / Methods** |
| --- | --- | --- |
| **1** | Obtain the latest APK or IPA file of the mobile application. | App download via device or directly from dev team. |
| **2** | Perform **static analysis** to extract app metadata, manifest, certificates, hardcoded URLs, endpoints, and services. | **MobSF, jadx, apktool** |
| **3** | Run the app on a device/emulator with a **proxy (Burp Suite)** intercepting traffic to capture all external communications. | Burp Suite, mitmproxy |
| **4** | Log in and navigate through all app features while capturing requests and responses. | Use test accounts where possible. |
| **5** | List all **domains, IP addresses, ports, API paths, cloud services, SDKs, and third-party integrations** communicating with the app. | Review proxy logs and static analysis reports. |
| **6** | Map out the architectural components: mobile client, backend servers, third-party APIs, CDN, authentication services, payment gateways, analytics platforms etc. | Diagram or tabular mapping |
| **7** | Review **permissions, exported components, API endpoints, data storage, and cryptographic implementation** in the app. | MobSF report, manual review |
| **8** | Identify all **security concerns** for each connected component/service. | Based on OWASP MASVS/MSTG and test results |