Mobile Application Pentesting Roadmap

Phase 1: Pre-engagement

- **Define Scope:**
  - Clearly define the scope of the mobile application penetration test, including target platforms (iOS, Android), app versions, and specific functionalities.
- **Legal and Compliance:**
  - Ensure compliance with legal and ethical standards. Obtain written permission from the app owner or organization.
- **Gather Information:**
  - Collect information about the mobile app, including its purpose, features, and any publicly available information. Review any relevant documentation.

Phase 2: Reconnaissance

- **Platform Analysis:**
  - Identify the target mobile platforms (iOS, Android) and their specific security considerations.
- **App Discovery:**
  - Enumerate mobile app endpoints, APIs, and server infrastructure.
- **Static Analysis:**
  - Conduct static analysis on the app binary to identify potential vulnerabilities and gather insights into its structure.

Phase 3: Dynamic Analysis

- **Dynamic Testing:**
  - Use dynamic analysis tools to identify runtime vulnerabilities, data storage issues, and communication security.
- **API Security Testing:**
  - Test the security of APIs used by the mobile app, including authentication, authorization, and data integrity.
- **Network Traffic Analysis:**
  - Monitor and analyze the app's network traffic to identify potential security issues and data leakage.

Phase 4: Code Review

- **Source Code Analysis:**
  - Perform a thorough review of the mobile app's source code, focusing on secure coding practices and potential vulnerabilities.
- **Third-Party Library Review:**
  - Assess the security of third-party libraries and dependencies used by the app.

Phase 5: Exploitation

- **Authentication Bypass:**
  - Attempt to bypass authentication mechanisms, including password-based and token-based systems.

- **Data Storage Exploitation:**
  - Exploit weaknesses in data storage, including insecurely stored data on the device or insecure data transmission.
- **Insecure Direct Object References (IDOR):**
  - Test for IDOR vulnerabilities, ensuring that user access controls are properly implemented.

Phase 6: Post-exploitation

- **Sensitive Data Exposure:**
  - Check for sensitive data exposure issues, such as the insecure transmission of personally identifiable information (PII).
- **Backdoor Testing:**
  - Test for the presence of backdoors or hidden functionalities that could pose a security risk.
- **Session Management:**
  - Assess the mobile app's session management mechanisms for weaknesses and potential session hijacking risks.

Phase 7: Reporting

- **Document Findings:**
  - Compile a detailed report outlining vulnerabilities, their severity, and potential impact.
- **Risk Prioritization:**
  - Prioritize findings based on risk and potential impact, providing recommendations for remediation.
- **Mitigation Strategies:**
  - Offer clear and actionable mitigation strategies to address identified vulnerabilities.

Phase 8: Debriefing

- **Client Debrief:**
  - Present findings and recommendations to the client. Discuss any additional insights gained during the testing.
- **Lessons Learned:**
  - Conduct an internal review to identify lessons learned and improve future testing processes.