Mobile_Application_Penetration_Testing_Theory

- **Introduction to Mobile Pentesting:**

Mobile application penetration testing focuses on identifying security weaknesses in Android and iOS applications, including insecure storage, weak authentication, improper platform usage, and runtime vulnerabilities.
Specifically: OWASP Mobile Top 10

- **OWASP Mobile Top 10 (Focus Areas):**

M1: Improper Platform Usage

Misuse of Android components

Exported activities

Misconfigured permissions

M2: Insecure Data Storage

Storing passwords in plaintext

Hardcoded API keys

Sensitive data in SharedPreferences

M3: Insecure Communication

No certificate pinning

HTTP instead of HTTPS

- **Static vs Dynamic Testing:**

1) **Static Analysis:** Static testing analyzes the APK file without running it.

Tool: MobSF

Used to:

- Check permissions
- Detect hardcoded secrets
- Find insecure storage
- Review manifest file

2) Dynamic Analysis: Dynamic testing analyzes the app while running.

Tool: Frida

Used to:

Hook functions

Bypass authentication

Modify runtime behavior

- **Secure Mobile Design:**

Explain mitigation techniques:

- Use encrypted storage
- Enable certificate pinning
- Obfuscate code
- Disable debugging in production
- Validate input properly

Frida was used to hook the application's authentication function at runtime. The return value was modified to bypass login verification. This demonstrates how insecure client-side validation can be manipulated dynamically, allowing attackers to gain unauthorized access without valid credentials.

A mobile security assessment was conducted on an Android application. Static analysis revealed insecure data storage issues. Dynamic testing using Frida demonstrated authentication bypass vulnerabilities. Improper exposure of application components was also observed. These findings highlight the risks of weak mobile security implementation.