# 📘 SEC575: iOS and Android Application Security Analysis & Penetration Testing

**Duration:** 6 Days | **8 Hours per Day**

---

## Day 1 – Mobile Security Foundations & Lab Setup

- Mobile threat landscape and real-world attack cases
- Android security architecture (apps, sandboxing, permissions)
- iOS security architecture (code signing, sandboxing, entitlements)
- Mobile penetration testing methodologies (OWASP MASVS, MSTG)
- Understanding mobile attack surfaces
- Setting up Android and iOS testing environments
- Emulator vs real device testing considerations

### Hands-On Labs

- Lab: Android emulator and iOS simulator setup
- Lab: Rooting Android / Jailbreaking iOS (lab environment)
- Lab: Mobile pentest toolkit installation and validation

---

## Day 2 – Reconnaissance & Static Analysis

- Mobile application reconnaissance techniques
- Application extraction techniques (APK, IPA)
- Android static analysis
  - Manifest analysis
  - Permissions review
  - Source code and resource analysis
- iOS static analysis
  - Info.plist review
  - Binary inspection
- Identifying hardcoded secrets and sensitive data

### Hands-On Labs

- Lab: Extract and decompile an Android APK

- Lab: Analyze Android app permissions and exposed components
- Lab: Static analysis of iOS app binary
- Lab: Identify hardcoded credentials and API keys

---

# Day 3 – Dynamic Analysis & Runtime Attacks

- Runtime behavior analysis concepts
- Dynamic instrumentation techniques
- Android dynamic analysis
- iOS dynamic analysis
- Root and jailbreak detection mechanisms
- Bypassing root/jailbreak detection
- Memory inspection and filesystem analysis

### Hands-On Labs

- Lab: Dynamic analysis using Frida and Objection
- Lab: Bypass root / jailbreak detection
- Lab: Runtime manipulation of app logic
- Lab: Inspect local files and memory artifacts

---

# Day 4 – Network Traffic & Backend API Attacks

- Mobile network communication architecture
- Intercepting mobile traffic
- SSL/TLS fundamentals in mobile apps
- Certificate pinning implementation and weaknesses
- Bypassing SSL/TLS pinning
- API security testing from mobile applications
- Backend integration vulnerabilities

### Hands-On Labs

- Lab: Intercept mobile traffic using proxy tools
- Lab: Bypass SSL/TLS certificate pinning
- Lab: Test mobile API authentication and authorization
- Lab: Identify backend API logic flaws

---

# Day 5 – Data Storage, Authentication & Platform Attacks

- Insecure local data storage risks
- Shared preferences, databases, keychains, keystores
- Token handling and session management flaws
- Biometric authentication security
- Insecure cryptographic implementations
- Secure storage best practices

### Hands-On Labs

- Lab: Extract sensitive data from local storage
- Lab: Analyze token and session handling
- Lab: Bypass weak biometric authentication
- Lab: Identify cryptographic implementation flaws

---

# Day 6 – Advanced Attacks, Anti-Tampering & Reporting

- Anti-tampering and anti-debugging techniques
- Code obfuscation and reverse engineering
- Bypassing integrity checks
- Professional mobile pentest reporting
- Risk rating and remediation guidance
- End-to-end mobile pentest workflow

### Hands-On Labs

- Lab: Bypass anti-debugging and integrity checks
- Lab: Reverse engineer protected mobile app logic
- Capstone Lab: Full mobile application penetration test
- Lab: Create professional pentest report

---

---