SL-MPTE – Mobile Penetration Testing Essentials

Course Syllabus

Course Overview

This course provides students with a complete, practical introduction to Mobile Application Penetration Testing, following **PTES**, **OWASP MASVS/MSTG**, and industry-standard methodologies.
Students will develop hands-on experience with static analysis, dynamic analysis, reverse engineering, API testing, and full mobile exploitation workflows.

Structure

- **Total Meetings**: 15
- **Format**: Instructor-led theory, guided labs (MobSF, Frida, Objection, Burp Suite, custom test apps), class missions, home missions, and self-investigate tasks.
- **Final Project**: Simulated mobile penetration test & reporting exercise.

SL-MPTE

Meetings Breakdown

Meet 1 – Introduction & Methodologies

- PTES phases for mobile
- MASVS & MSTG overview
- Lab setup: Android Studio, Genymotion, iOS jailbreak, MobSF

Meet 2 – Mobile Architecture & Fundamentals

- Android internals: APK, Dalvik/ART, manifest, permissions
- iOS internals: IPA, sandboxing, entitlements
- Secure app development flaws

Meet 3 – Recon & Static Analysis

- Tools: MobSF, JADX, strings
- Hardcoded secrets & sensitive data exposure
- Binary structure inspection

Meet 4 – Dynamic Analysis Basics

- ADB usage & traffic interception
- Proxy setup with Burp
- SSL pinning & bypass methods

Meet 5 – Authentication & Session Management

- Weak login flows & tokens
- Session fixation in mobile apps
- MFA & token storage flaws

Meet 6 – Data Storage & Cryptography

- Insecure storage: SharedPreferences, SQLite, iOS Keychain
- Weak cryptography usage
- Root/jailbreak detection bypass

Meet 7 – Reverse Engineering I (Android)

- Decompiled Java/Smali analysis
- Detecting insecure logic
- Obfuscation basics

Meet 8 – Reverse Engineering II (iOS)

- IPA structure & entitlements
- Jailbroken device testing
- Class-dump & binary inspection

Meet 9 – Network Traffic Analysis & MITM

- HTTP/HTTPS interception
- Certificate validation flaws
- Custom protocol abuse

Meet 10 – Input Validation & Injection

- SQLi, NoSQLi in mobile backends
- OS command injection
- Client vs server-side validation

Meet 11 – Business Logic in Mobile

- Workflow bypasses
- Parameter tampering
- Payment & subscription abuse

Meet 12 – API Testing for Mobile Backends

- REST & GraphQL API flaws
- BOLA & insecure serialization
- Mapping to OWASP API Top 10

Meet 13 – Mobile OS Exploitation Basics

- Root/jailbreak exploitation
- Privilege escalation flaws
- Misconfigured permissions

Meet 14 – Advanced Dynamic Testing

- Frida & Objection for runtime instrumentation
- Hooking methods & bypassing protections
- Memory dumping & advanced MITM

Meet 15 – Final Simulation & Reporting

- Full mobile PT engagement (end-to-end)
- Mapping findings to MASVS/MSTG
- Documentation & reporting best practices

Evaluation

- **Class Missions**: Practical in-class labs
- **Home Missions**: Individual assignments after each meet
- **Self-Investigate**: Independent research on standards & real-world cases
- **Final Project**: End-to-end mobile penetration test + report