Mobile Application Pentesting – Android Application Hacking

Module 1: Getting Started with Android Security

- Android Introduction
- Android System Architecture
- Security Bounds & Enforcement
    - Android Sandboxing
    - Android Permissions
- Android Layers
- The Android Framework
- The Dalvik Virtual Machine
- User-Space Native Code
- The Kernel
- Android Application Signing
- Android Startup Process

Module 2: MOBILE INFRASTRUCTURE: ARCHITECTURE COMPONENTS

- Virtual Private Networks (VPNs)
- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Identity and Access Management (IAM)
- Mobile Application Store (MAS)
- Mobile Application Gateway (MAG)
- Data Loss Prevention (DLP)
- Intrusion Detection System (IDS)
- Gateway and Security Stack (GSS)

Module 3: Setting Up the Environment

- Creating An Android Virtual Device
- Android PentestToolkit:
    - Android Debug Bridge
    - APK Tool
    - Burp Suite
- Getting Started with AppUse

Module 4: Reverse Engineering and Auditing Android Applications

- Android Application Teardown
- Reversing an Android Application
- Using APKtool to reverse an Android application
- Auditing Android Applications
- Content Provider leakage

Module 5: Mobile Applications Threats

- Insecure file Storage
- Path/Directory Traversal Vulnerability
- Local File Inclusion
- Remote File Inclusion
- Client-Side Injection Attacks
- Password Brute Force
- Unauthorized Dialing, SMS & payment
- OWASP Mobile Top 10
- Unsafe Sensitive data Storage
- Unsafe Sensitive data Transmission
- Cracking Screen Locks

Module 6: Application Penetration Testing

- Input Validation
- Buffer Overflow
- Cross Site Scripting
- URL Manipulation
- SQL Injection
- Hidden Variable Manipulation
- Cookie Modification
- Authentication Bypass
- Code Execution
- Injections
- Broken authentication and session management
- Cross-site scripting
- Insecure direct object references
- Security misconfiguration

- Sensitive data exposure
- Missing function level access control
- Cross-site request forgery
- Using components with known vulnerabilities
- Invalidated redirects and forwards

Module 7: Mobile Application Security Assessment and Penetration Testing

- Identify weaknesses in the default installation
- Bypass authentication and authorization mechanisms
- Escalate privileges
- Access and modify data or data presentation
- Attack vectors
- Data validation (SQL injection, Cross-Site Scripting, buffer overflows, etc.)
- Session management
- Access controls (authentication and authorization controls)Mobile Device Security Models
- Privilege and access models on multiple platforms
- Device encryption support and threats
- Bypassing passcode locks
- Decrypting credentials
- Accessing mobile device backup data
- Unlocking, Rooting, Jailbreaking Mobile Devices
- Mobile Phone Data Storage and Filesystem Architecture
- Filesystem Application Modeling
- Mobile application network capture
- Mobile app data extraction
- Exploiting SQL injection in mobile application frameworks
- CA Certificates

Module 8: Playing with SQLite

- Understanding SQLite in Depth
- Analyzing a simple application using SQLite
- Security Vulnerability

Module 9: Writing the Pentest Report

- Basic of a penetration testing Report
- Writing the Pentest Report
    - Executive Summary
    - Vulnerabilities
    - Scope of the work
    - Tools Used
    - Testing Methodologies followed
    - Recommendations
    - Conclusions