Android Application Penetration Testing Syllabus

- Module 1: Introduction
- Understanding the Basics of Android Penetration Testing
- Differentiating between Android Pentesting & Bug Bounty Approach

- Module 2: Understanding Android Application Attack Surface
- Types Android Application Attack Surface

- Module 3: Lab Environment Setup
- Genymotion Android Emulator Installation
- Installing Android App Components (GSuite)
- Installing Android App Components ARM Translator
- Android Pentesting Portable Integrated Environment

- Module 4: Android Debug Bridge Setup
- Setting up Android Debug Bridge

- Module 5: Delving into Android Architecture
- Overview of Android's Security Architecture
- Android Architecture
- Comparing Dalvik Virtual Machine (DVM) and Android Runtime (ART)

- Module 6: Android Application Compilation and Structure

- Understanding the Source Code Compilation Process
- Structure of an Android App

- Module 7: Unpacking and Reversing Android Applications
- Unzipping and Unpacking Android Applications
- Reversing an Android Application using dex2jar
- Reversing an Android Application using apktools
- Jdgui

- Module 8: Manifest and Signing Android Applications
- Android Application Manifest Overview
- Manual and Automated Signing of Android Applications

- Module 9: Source Code Analysis and Protection
- Understanding Code Obfuscation and Code Protection
- Conducting Static Source Code Analysis
- Understanding the android-debug

- Module 10: Dynamic Security Analysis
- Steps for Dynamic Security Analysis of Application
- Utilizing Drozer Security Testing Framework for Dynamic Security Analysis
- Performing Dynamic Security Analysis using BurpSuite

- Module 11: Common Android Security Issues
- Insecure Protocols
- Insecure Logging Security Issues

- Insecure Sensitive Hardcoding Issues
- Cryptographic Storage Issues: Shared Preferences, SQLite, Internal Storage
- Addressing Application Level Denial-of-Service
- Recognizing Insecure Backup Storage
- Sensitive Data Copied to Clipboard

- Module 12: OAuth Tokens and 2FA
- Understanding Leaking OAuth Tokens in Android logcat
- Insecure Authentication and Authorization
- Bypassing Second Factor Authentication (2FA)

- Module 13: Application Vulnerabilities and Exploits
- Insecure Direct Object References (IDOR)
- Local File Inclusion
- Improper Session Handling

- Module 14: Penetration Testing Report
- Android Penetration Testing Report - Test Cases