ANDROID PENTESTING COURSE – SYLLABUS DETAILS

What you will learn

Chapter 1: Android Fundamentals

- 1.1 History of Android
- 1.2 Understanding Android Hardware and Software Architecture
- 1.3 Android OS Versions and Compatibility
- 1.4 Android Security Model
- 1.5 Android Permission Model for Application Security
- 1.6 Sandboxing and Device Rooting
- 1.7 Understanding SELinux and App Security
- 1.8 Securing Android with Google Play Protect

Chapter 2: iOS Fundamentals

- 2.1 History of iOS
- 2.2 Understanding iOS Hardware and Software Architecture
- 2.3 iOS OS Versions and Compatibility
- 2.4 iOS Security Model
- 2.5 iOS Permission Model for Application Security
- 2.6 Sandboxing and Device Jailbreaking
- 2.7 Understanding Apple's Secure Enclave
- 2.8 App Store Security Standards

Chapter 3: Mobile App Security Basics

- 3.1 Understanding APK and IPA Package Structures
- 3.2 Key Directories and Files in APK/IPA Packages
- 3.3 Codesigning and Application Encryption
- 3.4 Mobile App Security Threat Landscape
- 3.5 Android and iOS App Stores: Security Requirements and Policies
- 3.6 Mobile App Hardening Techniques

What you will learn

Chapter 4: Mobile Application Vulnerabilities

- **4.1 Weak Server-Side Controls (M1): Understanding and Exploiting**
- **4.2 Insecure Data Storage (M2): Risks and Mitigations**
- **4.3 Insufficient Transport Layer Protection (M3): Exploiting and Fixing**
- **4.4 Unintended Data Leakage (M4): Vulnerabilities in Caches and Logs**
- **4.5 Poor Authentication & Authorization (M5): Types and Avoidance**
- **4.6 Broken Cryptography (M6): Symmetric, Asymmetric & Key Management**
- **4.7 Client-Side Injections (M7): Testing for XSS and SQLi on Mobile**
- **4.8 Security Decisions via Untrusted Input (M8): Common Risks**
- **4.9 Improper Session Handling (M9): Session Management in Mobile Apps**
- **4.10 Lack of Binary Protection (M10): Reverse Engineering and Patching**
- **4.11 Additional Vulnerabilities: Intent Spoofing, Tapjacking, and Side-Channel Attacks**

Chapter 5: Setting up Mobile Pentesting Environment

- **5.1 Mobile Pentesting Setup for Android and iOS**
- **5.2 Device Emulators and Simulators for Testing**
- **5.3 Rooting and Jailbreaking for Research Purposes**
- **5.4 Using Drozer for Android Security Testing**
- **5.5 Analyzing AndroidManifest.xml and App Permissions**
- **5.6 Configuring Burp Suite for Traffic Interception**
- **5.7 Bypassing Traffic Interception Protections**
- **5.8 Working with Frida for Dynamic Instrumentation**
- **5.9 Static and Dynamic Analysis Tools Setup**

What you will learn

Chapter 6: Mobile Application Attacks

- 6.1 Exploiting Android and iOS Vulnerabilities
- 6.2 Penetration Testing Workflow and Methodologies
- 6.3 Essential Mobile Security Testing Tools (MobSF, QARK, OWASP ZAP)
- 6.4 Techniques for Bypassing Security Controls (SSL Pinning, Root Detection)
- 6.5 Dynamic Analysis and Hooking with Xposed and Frida
- 6.6 Reverse Engineering Android and iOS Apps
- 6.7 Working with Proxies and Analyzing API Calls
- 6.8 API Security Testing in Mobile Applications

Chapter 7: Advanced Mobile Application Attacks

- 7.1 Advanced Exploitation Techniques and Tools
- 7.2 Bypassing Multi-Layered Security Controls
- 7.3 Advanced Dynamic Instrumentation for Vulnerability Analysis
- 7.4 Mobile Device Forensics and Data Recovery Techniques
- 7.5 Exploiting Zero-Day Vulnerabilities in Mobile Apps
- 7.6 Advanced Reverse Engineering with IDA Pro and Ghidra

Chapter 8: Mobile Pentesting Best Practices

- 8.1 Comprehensive Mobile Pentesting Methodologies
- 8.2 Mobile App Security Testing Frameworks (OWASP MASVS, MSTG)
- 8.3 Recommended Tools for Professional Mobile Pentesters
- 8.4 Reporting and Documentation Best Practices
- 8.5 Effective Vulnerability Disclosure and Communication

ANDROID PENTESTING COURSE – SYLLABUS DETAILS

What you will learn

Chapter 8: Mobile Pentesting Best Practices

- 8.1 Comprehensive Mobile Pentesting Methodologies
- 8.2 Mobile App Security Testing Frameworks (OWASP MASVS, MSTG)
- 8.3 Recommended Tools for Professional Mobile Pentesters
- 8.4 Reporting and Documentation Best Practices
- 8.5 Effective Vulnerability Disclosure and Communication
- 8.6 Mobile Security Compliance and Standards (PCI DSS, GDPR)

Chapter 9: Mobile CTF Challenges and Labs

- 9.1 Basic Android CTF Challenges: Reverse Engineering and Permissions Bypass
- 9.2 Advanced Android CTFs: Exploiting Insecure Data Storage and SSL Pinning Bypass
- 9.3 Basic iOS CTF Challenges: Jailbreaking and Binary Analysis
- 9.4 Mixed Mobile CTFs: Multi-Platform Challenges on API Security
- 9.5 Capture the Flag Labs: Real-World Scenarios and Vulnerability Exploitation
- 9.6 Guided Walkthroughs for CTF Challenges and Solutions