CA203: Mobile Penetration Testing

15 Instructional Hours 27 CPEs 12 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER TO INTERMEDIATE

This course provides a comprehensive and practical exploration of mobile application penetration testing, focusing on both Android and iOS platforms. It covers foundational concepts such as mobile security threats, operating system architectures, and security models, before progressing into hands-on techniques for identifying and exploiting vulnerabilities. Learners will gain experience in setting up a professional pentesting environment, performing static and dynamic analysis, intercepting network traffic, and applying OWASP Mobile Security guidelines. The course emphasizes real-world attack vectors, tools, and methodologies used by security professionals to assess and secure mobile applications in modern threat landscapes.

You Will Be Able To

- Analyze mobile application architectures (Android and iOS) to identify potential security weaknesses
- Perform static and dynamic analysis on mobile applications using industry tools
- Capture and inspect network traffic to detect insecure communications and vulnerabilities
- Identify and exploit common mobile vulnerabilities aligned with OWASP Mobile Top 10
- Set up and configure a complete mobile pentesting environment using tools like Genymotion, ADB, and Burp Suite
- Assess mobile applications against real-world attack vectors including insecure storage, authentication flaws, and data leakage

Who Should Attend

This course is designed for cybersecurity professionals, penetration testers, and developers who want to build or strengthen their expertise in mobile application security. It is also suitable for IT professionals and security enthusiasts seeking practical, hands-on experience in identifying and mitigating vulnerabilities in Android and iOS applications. A basic understanding of networking, operating systems, and security concepts is recommended for optimal learning outcomes.

Relevant Combat Roles

- Mobile Application Penetration Tester
- Cybersecurity Analyst (Mobile Security Focus)
- Red Team Operator
- Security Engineer (Application Security)
- Vulnerability Researcher
- Mobile Security Consultant

Topics Covered

Fundamentals of mobile penetration testing, threat landscape, and common attack vectors (data at rest/in motion, device-level threats)

Android & iOS security: architecture, sandboxing, security models, rooting and jailbreaking concepts

Setting up pentesting environments (Genymotion, Android Studio, ADB) and app deployment/debugging techniques

Network traffic analysis using tools like Burp Suite and proxy configurations

Static & dynamic analysis: APK decompilation (JADX, APKTool, MobSF), Frida, drozer, and runtime/log analysis

OWASP Mobile Top 10 risks, secure development practices, and real-world exploitation scenarios

Labs

Mobile Pentesting Lab Setup & Android Testing Environment
(Genymotion installation, Android Studio integration, Android SDK configuration, ADB setup, emulator deployment, and virtual device management for mobile security testing)

Android Application Deployment & Device Interaction
(Deploying APKs to Genymotion using ADB, drag-and-drop installation, emulator connectivity, and Android Debug Bridge workflows)

Android Static Analysis & Reverse Engineering
(Decompiling APKs, JADX usage, APKTool analysis, identifying hardcoded secrets, insecure storage, binary protections, and reverse engineering Android applications)

Mobile Traffic Interception & API Security Testing
(Burp Suite proxying, network traffic interception, insecure communication analysis, API attack-surface mapping, authentication testing, session management testing, and OWASP Mobile Top 10 validation)

Android Dynamic Analysis & Runtime Instrumentation
(Using Frida for runtime manipulation, dynamic hooking, SSL pinning bypass, drozer deployment, runtime testing, log analysis with Logcat, and behavioral analysis of Android applications)

Mobile Vulnerability Assessment & Exploitation Techniques
(Analyzing insecure communication, insecure storage, weak cryptography, security misconfigurations, certificate pinning bypass, deep link abuse, and advanced mobile attack vectors)