COURSE OUTLINE

ETHICAL HACKING
Certified Mobile Security Tester (CMST)

SPECIALIST-LEVEL COURSE Cost: **£1,950.00** + VAT Duration: **3 days**

This three-day course is for people in a wide variety of mobile application-related roles. It introduces the fundamentals of mobile application security and gives you an understanding of whether the sensitive information stored on mobile devices is sufficiently protected.

COURSE OVERVIEW

Focussing on the prevalent mobile platforms, Android and iOS, you will have access to vulnerable mobile applications using devices and emulators to assess their security through a series of practical hands-on exercises. The techniques gained throughout this course will enable you to understand whether the sensitive information stored on mobile devices is sufficiently protected and what the risk and exposure is if an attacker was able to get his hands on the mobile device.

THE SKILLS YOU WILL LEARN

- You will be led through the current OWASP Mobile Top Ten, the most critical mobile application security risks that leave organisations and their customers' data vulnerable to attack
- Once able to identify and exploit vulnerabilities in both iOS and Android platforms, you will be introduced to a range of defensive countermeasures, allowing you to develop applications that are more resistant to attack
- Understand where issues might appear in a mobile application and the significance of data stored on every day mobile devices
- Have learnt to retrieve class methods by reverse engineering iOS applications and gained the ability and confidence to reverse engineer Android applications to obtain source code
- Have learnt the fundamental vulnerabilities found on mobile applications, including static and runtime analysis of the applications, insecure data storage and binary patching.

KEY BENEFITS

This course will give you:

- An understanding of whether the sensitive information stored on mobile devices is sufficiently protected and what the risk would be if the device fell into the hands of an attacker
- The ability to use a variety of tools and techniques, including static and run-time analysis, binary patching and reverse engineering, to improve mobile application security

WHO SHOULD ATTEND

Anyone looking to understand the fundamentals of mobile application security, including:

- App developers
- IT security officers
- Penetration testers
- Network and systems administrators

PREREQUISITES

A basic understanding of:

- How the iOS and Android platform and devices work
- HTTP protocol
- Programming
- Windows and Linux command line
- Java and Objective-C languages

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Mobile Security Tester (CMST) qualification.

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com

COURSE OUTLINE

ETHICAL HACKING
Certified Mobile Security Tester (CMST)

SPECIALIST-LEVEL COURSE | Cost: £1,950.00 + VAT | Duration: **3 days**

"The whole course was excellent, I did not realise what a massive and interesting field security is. It has opened my eyes to what the hackers do to try and steal sensitive data."

CMST Delegate Z-Tech Control Systems Ltd

SYLLABUS

1. **Security**
   a. iOS Security
      – Secure Boot Chain
      – Sandboxing
      – File security
   b. Android Security
      – Zygote
      – Sandboxing
      – File Access

2. **Application types: Native, Web based, Hybrid (Both)**

3. **Jailbreaking**

4. **Data in Transit**
   a. Setting up a proxy (Both)
   b. Installing certificates
   c. Certificate Pinning (Both)
   d. SQL injection (Both)
   e. XSS (Both)
   f. URL Schemes
   g. Content Providers (Android)
   h. Javascript Bridges (Android)

5. **Data at Rest**
   a. SQLite files (Both)
   b. Plist files
   c. NSUserDefaults
   d. Core Data
   e. Keychain
   f. Cookies
   g. Data location (Android)

6. **Static Analysis**
   a. Decrypting Applications
   b. Position Independent Executable (PIE) Flag
   c. Class Dumping
   d. Binary patching
   e. Automated Tools (Both)
   f. Manifest file examination (Android)
   g. Reverse Engineering (Android)
   h. Smali code syntax (Android)
   i. Java decompilation (Android)
   j. Hardcoded sensitive information (Android)
   k. Application backups (Android)
   l. Broken Cryptography (Android)

7. **Dynamic Analysis/Runtime Analysis**
   a. Runtime Patching (Both)
   b Runtime Manipulation
   c. Automated Tools
   d. Activity manager (Android)
   e. Reflection (Android)

8. **Side Channel Attacks**
   a. Screenshots
   b. Cookies (Android)
   c. Cache (Both)

9. **Known attacks**
   a. Known attacks
   b. Cache

PA Consulting
Global Innovation & Technology Centre
Back Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
www: cybereducation.paconsulting.com

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com